Quelques réflexions juridiques sur l'administration électronique

Burton, Cedric; Poullet, Yves

Published in:
Quand l'informatique rencontre l'action sociale...

Publication date:
2007

Document Version
le PDF de l'éditeur

Quelques réflexions juridiques sur l'administration électronique : le cas des CPAS

Cédric BURTON, Yves POULLET

Introduction

S'il est un lieu commun de considérer qu'Internet, les réseaux et autres technologies de l'information et de la communication prennent de plus en plus de place dans notre société, que chaque citoyen, chaque personne morale, chaque administration est confrontée au monde de l'informatique, rares sont les réflexions sur les risques que véhiculent ces « nouvelles technologies ». En effet, cette incursion de l'informatique dans notre quotidien nous est principalement présentée comme une « solution miracle » permettant de résoudre certains maux dont souffre notre administration. Il est malheureusement souvent omis de mentionner les dangers que représentent ou peuvent représenter ces avancées technologiques.

Au rang des avantages généralement décris et perçus par l'arrivée de l'informatique et du numérique dans l'administration figurent principalement les soucis d'efficience et de contrôle des administrés[1]. Si ces avantages semblent indéniables, d'aucuns oublient souvent que cette administration électronique doit offrir certaines garanties au citoyen telles que la protection de leur vie privée, le secret de leur correspondance, une transparence dans le fonctionnement administratif et un accès à l'information publique. Grâce aux technologies de l'information et en vertu du principe de réciprocité des avantages, ces garanties devraient même se voir renforcées[2]. Signalons également d'emblée que certains principes

[1] Voy. sur ce point C. BURTON, V. LAURENT, C. LOBET-MARIS, F. NAVARRE, Y. POULLET, L'informatisation des CPAS, une informatique plurielle au service de l'action sociale – Résultats du questionnaire préparatoire au Colloque des Secrétaires de CPAS, Avril 2006, Herbeumont, disponible sur http://www.fundp.ac.be/pdf/publications/57376.pdf

[2] A propos du principe de réciprocité des avantages, voy. Y. POULLET, « Mieux sensibiliser les personnes concernées ; les rendre acteurs de leur propre

fondateurs de nos sociétés démocratiques, tels que les principes de non discrimination, de vie privée ou d'auto-détermination[3], risquent également d'être mis à mal si notre attention ne reste pas soutenue…

La prolifération des réseaux, la multiplication des collectes de données, leur conservation et leur interconnexion sans cesse facilitées constituent autant de risques d'atteinte à la vie privée de tout un chacun. Ainsi, l'enquête menée conjointement par la CITA et la CRID montre que 54% des CPAS disposent d'un dossier informatisé unique par « client », mêlant les données collectées à l'occasion des divers services que le CPAS peut offrir à ces usagers comme les repas à domicile, les cours d'initiation à l'informatique, le logement social, les allocations de subsistance, Vis-à-vis de tels fichiers, les règles d'accès développées par la plupart des CPAS sont dérisoires. Au-delà de cette réflexion sur le fichier dit unique, on note que chacun des services offerts par le CPAS justifie un traitement de données à caractère personnel dont certaines peuvent être sensibles.

La présence grandissante des traitements de données à caractère personnel dans la gestion des activités des CPAS et la nécessaire protection de ces données constitueront, la première partie de cette contribution. Elle se focalisera sur la protection de la vie privée et

protection, Rapport établi pour la conférence du Conseil de l'Europe, organisé à Prague, les 14 et 15 octobre 2004 », *Revue Lamy Droit de l'Immatériel*, 2005, N°5, pp.47 – 57. L'idée centrale est la suivante : dans la mesure où l'administration ou plus largement les responsables de traitement bénéficient grâce aux techniques de traitement de l'information de facilités plus grandes dans la gestion de leurs opérations et tirent de cette technologie d'incontestables avantages et réductions de coût, il est de leur devoir de permettre aux personnes concernées de bénéficier elles aussi des avantages des technologies dans l'exercice de leurs droits (ainsi, l'accès électronique aux données, la possibilité à travers les logfiles ou journaux de bord des accès au système d'information, de connaître la liste des personnes ayant consulté leurs données, etc.

[3] Sur ce concept développé par la jurisprudence de la Cour européenne des droits de l'Homme et d'autres cours constitutionnelles, nos remarques infra Titre I, 1.

plus particulièrement sur la protection des données à caractère personnel. Dans le titre II, seront ensuite formulées

quelques réflexions sur le secret de la correspondance ou, plus largement des communications électroniques.

Le titre III analyse quelques questions juridiques relatives à la gestion des moyens informatiques, en particulier en lien avec la mutualisation de ces moyens. Le titre IV aborde les questions liées à l'utilisation de l'électronique par et à l'attention des CPAS. Les exigences du formalisme *« ad probationem »* et *« ad validatem »* face au numérique seront abordées. Finalement, le titre V se penche sur les raisons et les différentes manières de créer une charte informatique au sein des CPAS.

Section I
La protection de la vie privée

Introduction

Une multitude de normes protègent la vie privée des individus, des citoyens. Au niveau international, la Convention européenne de sauvegarde des Droits de l'Homme et des Libertés fondamentales[4] est la plus célèbre. Mentionnons également l'article 17 du Pacte international relatif aux droits civils et politiques.[5] Depuis peu, la Charte européenne des Droits fondamentaux consacre la protection de la Vie privée dans son article 7[6]. En Belgique, l'article 22 de la Constitution garantit le droit au respect de la vie privée et familiale.

Au sein de l'ensemble de ces textes dits de protection de la vie privée, il est possible d'isoler également un nombre important de textes relatifs à ce que l'on appelle communément la protection des données à caractère personnel, qui ne représente qu'une facette de la vie privée et familiale consacrée par l'article 8 de la Cours Européenne des Droits de l'Homme (CEDH). Ainsi, on cite la Convention n° 108 du Conseil de l'Europe[7], l'article 8 de la Charte

[4] Ci après CEDH, disponible sur http://www.echr.coe.int/echr

[5] Cet article stipule que *« 1. Nul ne sera l'objet d'immixtions arbitraires ou illégales dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes illégales à son honneur et à sa réputation. 2. Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes. »*

[6] Cet article 7 stipule que « *Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de ses communications.* ». La charte est disponible à l'adresse suivante : http://www.europarl.europa.eu/charter/pdf/text_fr.pdf

[7] Convention n° 108 du conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, 28 janvier 1981, Strasbourg, disponible sur http://conventions.coe.int/Treaty/FR/Treaties/Html/108.htm

des Droits fondamentaux de Union Européenne, les directives 1995/46/CE[8] et 2002/58/CE[9] et en Belgique la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel[10] et son arrêté d'application du 13 février 2001[11] .

D'autres législations sectorielles visent également à réglementer les traitements de données à caractère personnel tels que la loi sur la Banque Carrefour de la sécurité sociale[12] (BCSS), la loi sur la centrale des crédits aux particuliers[13], la loi instaurant un registre national[14] des personnes physiques ou encore la loi sur la Banque Carrefour des entreprises[15], etc.

[8] Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, *J.O.C.E.*, 23 novembre 1995, L 281, p.31 à 50, disponible sur http://europa.eu.int/eur-lex/fr/index.html

[9] Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques), J.O.C.E., 31 juillet 2002, L 201, p.37 à 47, disponible sur http://europa.eu.int/eur-lex/fr/index.html

[10] Loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, *M.B.*, 18 mars 1993, p. 05801. *« LVP »* ci après.

[11] *M.B.,*13 mars 2001

[12] Loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque Carrefour de la sécurité sociale, *M.B.*, 22 février 1990, p. 03288.

[13] L. du 10 août 2001 relative à la Centrale des Crédits aux Particuliers, *M.B.*, 25 septembre 2001, p. 32027 et A.R. du 07 juillet 2002 réglementant la Centrale des Crédits aux Particuliers, *M.B.*, 19 juillet 2002.

[14] Loi du 8 août 1983 organisant un registre national des personnes physiques, *M.B.*, 21 avril 1984.

[15] Loi du 16 janvier 2003 portant création d'une Banque-Carrefour des Entreprises, modernisation du registre de commerce, création de guichets-entreprises agréés et portant diverses dispositions, *M.B.*, 5 février 2003.

Dans un premier temps notre attention se portera sur la notion de vie privée telle que progressivement définie et protégée au niveau européen.

Ensuite, nous nous focaliserons sur la protection qu'accordent à la fois la Constitution et la loi du 8 décembre 1992 sur les traitements de données à caractère personnel. Cette analyse sera l'occasion de familiariser le lecteur avec les notions clés de la protection des données à caractère personnel.

Troisièmement, nous profiterons de l'occasion pour formuler quelques réflexions sur l'intégration des CPAS au sein de la BCSS et tracerons les grands traits de cette législation.

1. La vie privée vue de l'Europe

Tout commence lorsqu' est inscrit en 1950 à l'article 8 de la Convention Européenne de Sauvegarde des Droits de l'homme et des libertés fondamentales (CEDH) que « *Toute personne a droit au respect de la vie privée et familiale, de son domicile et de sa correspondance* ». La CEDH ne précise pas ce qu'il faut entendre par vie privée et familiale. La signification du contenu de cette notion fut laissée à l'interprétation de la Cour Européenne des Droits de l'Homme qui en fit un concept souple et évolutif[16].

Si au départ cette protection se limitait à l'intimité des individus[17] contre de possibles incursions de l'Etat, la notion de vie privée a subi une double évolution, c'est-à-dire une augmentation du champ de la notion et une création de la doctrine des obligations positives.

[16] Pour consulter la jurisprudence de la Cour Européenne des Droits de l'Homme voy. http://www.echr.coe.int/ECHR/FR/Header/Case-Law/Hudoc/Hudoc+database

[17] Au départ la notion se comprenait comme « the right to be left alone », selon la formule célèbre des juges Brandeis et Warren prononcée en 1890 à propos d'une affaire relative à la publication d'informations par des journalistes (The right to privacy, 4 *Harv. Law Journal,* 183 (1890)

Le champ de la notion européenne de vie privée a connu une extension incroyable. C'est ce qu'exprime la Cour européenne des droits de l'homme lorsqu'elle écrit que « *La vie privée est une notion large, qui ne se prête pas à une définition exhaustive* »[18]. A l'heure actuelle, la vie privée comprend une multitude de réalités, de facettes de notre personnalité. Ainsi le secret de la correspondance[19], l'inviolabilité du domicile, la vie affective, les relations parents-enfants, voire grands-parents petits-enfants, l'orientation sexuelle, le droit à l'intégrité physique et morale, le droit de connaître ses origines, le droit à une conversion sexuelle, etc. sont autant d'aspects couverts par cette notion extrêmement large qu'est la vie privée. Cette extension est telle qu'aujourd'hui une part importante de la doctrine plaide pour une conception de la vie privée en tant que droit à l'autodétermination[20].

Toujours à propos du champ de la notion de vie privée, il faut insister sur le fait que cette notion ne se limite pas au cercle de famille ni aux « quatre coins du domicile familial ». Ainsi, la Cour reconnaît que chacun dispose d'une vie privée lorsqu'il « se balade en rue », dans le cadre de son travail, de ses relations professionnelles ou commerciales. Dans les mots de la Cour cela donne *« Il serait (...) trop restrictif de (...) limiter [La vie privée] à un « cercle intime » où chacun peut mener sa vie personnelle à sa guise et d'en écarter entièrement le monde extérieur à ce cercle. Le respect de la vie privée doit aussi englober, dans une certaine mesure, le droit pour l'individu de nouer et de développer des relations avec ses semblables. Il paraît, en outre, n'y avoir aucune raison de principe de considérer cette manière de comprendre la notion de « vie privée » comme excluant les activités*

[18] Voy entre autres, C.E.D.H., Arrêt Peck c. Royaume-Unis, 17 juillet 2003, §57 ; C.E.D.H., Arrêt Raninen c. Finlande, 16 décembre 1997, §63 ; C.E.D.H., Arrêt K.A. et A.D. c. Belgique, 17 février 2005, §79 ; C.E.D.H., Arrêt Wisse c. France, 20 décembre 2005, §24 ; C.E.D.H., Arrêt Niemietz c. Allemagne, 16 décembre 1992, §29 ; C.E.D.H., Arrêt Castello-Roberts c. Royaume-Uni, 25 mars 1993, §36 ; CE.D.H., Arrêt Bensaid c. Royaume-Uni, 6 février 2001, §47.

[19] En effet au niveau européen, il n'existe pas une norme particulière protégeant la correspondance comme c'est le cas en Belgique.

[20] Sur cette explosion du contenu de la « vie privée », lire « *Le droit au respect de la vie privée au sens de la Convention européenne des droits de l'homme »,* F.SUDRE (ed.), Coll. Droit et Justice, n° 63, Bruylant, 2005.

professionnelles ou commerciales : après tout, c'est dans leur travail que la majorité des gens ont beaucoup, voire le maximum d'occasions de resserrer leurs liens avec le monde extérieur. Il existe donc une zone d'interaction entre l'individu et autrui qui, même dans un contexte public, peut relever de la vie privée » [21]. Remarquons que tout individu a droit au respect de sa vie privée pendant les heures de travail que celles-ci soient prestées au bureau, ou soient prestées à l'extérieur comme cela est par exemple le cas des représentants de commerce, des aides soignantes et autres[22].

L'autre évolution majeure de la notion de vie privée réside dans la reconnaissance par la Cour européenne des Droits de l'Homme de la doctrine des obligations positives[23]. Alors que la notion d'obligation négative signifie que l'Etat ne peut s'immiscer dans la vie privée des individus[24], la notion d'obligation positive l'oblige à garantir à chaque individu le respect de sa vie privée y compris vis-à-vis de tiers, entreprises privées ou associations. Cela signifie que l'Etat fédéral et les entités fédérées doivent respecter la vie privée des individus en instaurant des normes la protégeant directement mais aussi en respectant cette liberté fondamentale lors de l'élaboration de toute autre norme. Ainsi, si l'Etat ne peut pas s'immiscer dans la vie privée des individus en réalisant lui-même des écoutes téléphoniques et ce au vu de ses obligations négatives, les obligations positives mises à charge de l'Etat signifient que, parallèlement, l'Etat doit prendre des mesures raisonnables et proportionnées afin d'empêcher les écoutes téléphoniques au sein des entreprises privées ou par les entreprises de communications

[21] Voy. les arrêts cités en note 15.

[22] Nous pensons par exemple ici aux questions liées à la géolocalisation des employés. Pour plus de détails, voy. le site de la CNIL : www.cnil.fr et plus spécialement le dossier sur la géolocalisation disponible à l'adresse :http://www.cnil.fr/fileadmin/documents/approfondir/dossier/geolocalisation/Guide-geolocalisation.pdf

[23] Sur ce point parmi de nombreux auteurs, F. SUDRE, « La doctrine des obligations « positives » dans la jurisprudence européenne des droits de l'homme », *Rev. Trim. des Droits de l'Homme*, 1995, p. 363.

[24] Sauf si la mesure est conforme à l'article 8 §2 de la CEDH, voy. le paragraphe suivant.

électroniques, par exemple en créant une législation incriminant ce comportement.

Cependant, la vie privée n'est pas un droit absolu. Ainsi, des ingérences peuvent exister si certaines conditions sont respectées. Le paragraphe 2 de l'article 8 CEDH prévoit les conditions permettant une atteinte à la vie privée des individus : *« Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui. »*

Une ingérence dans la vie privée est donc permise si premièrement elle est prévue par la loi au sens matériel[25] du terme c'est à dire par toute règle de droit d'application générale et impersonnelle présentant des qualités d'accessibilité, de prévisibilité et ayant un niveau de précision suffisant. Deuxièmement cette ingérence doit rencontrer l'un des objectifs prévus à l'article 8 §2 de la CEDH. Remarquons que ces objectifs sont assez larges et qu'il est relativement aisé de rentrer dans une de ces catégories. Finalement, la mesure doit être proportionnée à l'objectif poursuivi. Ce test de proportionnalité signifie qu'il faut mettre en balance d'une part la vie privée des individus et d'autre part l'objectif poursuivi par la mesure portant atteinte à la vie privée. Ainsi par exemple, il serait proportionné que l'Etat réalise des écoutes téléphoniques dans un objectif de lutte contre le terrorisme[26] sans doute sans que cela signifie une écoute systématique de tous les Belges mais simplement dans le cadre d'investigations en présence de personnes suspectes. En toute hypothèse, le principe de

[25] Peu importe que cette norme soit une loi formelle, un AR, une circulaire ou même de la jurisprudence.

[26] Il faut toutefois nuancer en précisant que la mesure devra être également la moins attentatoire possible à la vie privée et que les écoutes devront s'entourer de garanties suffisantes pour protéger dans la mesure du possible la vie privée des individus. Au minimum, des mesures de sécurité efficace et adéquate devront être prises pour empêcher le vol ou la réutilisation de ces données dans d'autres finalités.

proportionnalité exclut que les mêmes écoutes soient réalisées dans le but de surveiller voire d'incriminer des personnes exprimant pacifiquement des vues opposées à celles du gouvernement en place.

Les différentes considérations qui précèdent ont eu pour objet la Convention Européenne de sauvegarde des droits de l'homme et des Libertés fondamentales et ont pour champ d'application l'ensemble des pays membres du Conseil de l'Europe. Or, au sein du Conseil de l'Europe, l'Union Européenne a créé également un ensemble normatif de protection de la vie privée et des données à caractère personnel. Par choix, la Charte des droits fondamentaux ne fera pas l'objet d'analyse dans la présente contribution. Remarquons cependant qu'au sein de cette charte, appelée à devenir partie intégrante de la Constitution européenne, une disposition protège la vie privée et qu'une autre protège les traitements de données à caractère personnel. Actuellement les deux notions semblent donc diverger. Commet comprendre cette divergence de base légale ? La protection des données lors de leurs traitements serait-elle plus qu'une sous-division de la vie privée ? L'autodétermination informationnelle serait-elle plus qu'une sous-division de l'autodétermination ? Faut-il concevoir différemment les deux régimes de protection ou le Constituant européen a-t-il juste voulu « enfoncer le clou » et mettre sur un pied d'égalité la protection des données et la vie privée ?

L'Europe a consacré la protection des données à travers deux directives européennes. La première, la directive 95/46/CE relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données[27] s'applique de manière générale à tout traitement de données à caractère personnel automatisé. La loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel en est la transposition. Quant à la directive 2002/58/CE concernant le traitement des données à caractère personnel et la protection de la

[27] Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, *J.O.C.E.*, L 281 du 23 novembre 1995.

vie privée dans le secteur des communications électroniques,[28] elle crée certaines règles particulières pour les traitements de données dans le domaine des communications électroniques et fut transposée dans la loi du 13 juin 2005 sur les communications électroniques. Ces deux directives étant pour l'essentiel identiques à leur transposition belge, nous ne nous y attarderons pas mais concentrerons notre attention sur la législation belge.

2. La vie privée en Belgique

L'article 22 de la Constitution relaie en droit Belge l'article 8 de la CEDH : *« Chacun a droit au respect de sa vie privée et familiale, sauf dans les cas et conditions fixés par la loi. La loi, le décret ou la règle visée à l'article 134 garantissent la protection de ce droit. ».*

Il ressort des travaux préparatoires de l'article 22 de la Constitution que « le Constituant a cherché la plus grande concordance possible avec l'article 8 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, afin d'éviter toute contestation sur le contenu respectif de l'article de la Constitution et de l'article 8 de la Convention »[29], ce qui suppose que la jurisprudence constitutionnelle belge suivra les avancées de la cour strasbourgeoise..

A première vue, cet article présente donc de fortes similarités avec l'article 8 de la CEDH. Il faut néanmoins souligner quelques divergences : (1) les ingérences ne peuvent avoir lieu que si elles sont prévues par la loi au sens formel du terme c'est à dire par une disposition législative[30]. De plus cette loi doit en principe émaner du

[28] Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques), *J.O.C.E.,* L 201 du 31 juillet 2002.

[29] C.A., n° 16/2005, 19 janvier 2005, B.2.4. et Doc. parl., Chambre, 1993-1994, n° 997/5, p. 2.

[30] Voy. notamment, D. DE ROY, C. de TERWANGNE, Y. POULLET, La convention européenne des droits de l'homme en filigrane de l'administration

pouvoir fédéral. *« En effet, seul le législateur fédéral peut déterminer dans quels cas et à quelles conditions le droit au respect de la vie privée et familiale peut être limité. »*[31] *Les entités fédérées peuvent créer une ingérence dans la vie privée dans le cadre de leurs compétences respectives mais à condition de respecter le cadre général que constituent les normes fédérales. C'est ce qu'exprime la Cour d'arbitrage lorsqu'elle écrit qu' « une ingérence dans la vie privée qui s'inscrit dans la réglementation d'une matière déterminée relève certes du législateur compétent pour régler cette matière, mais le législateur décrétal est tenu de respecter la réglementation fédérale générale, qui a valeur de réglementation minimale pour toute matière. »*[32] (2)

Par contre, la deuxième phrase de cet article 22 prévoit explicitement la possibilité pour l'Etat fédéral et les entités fédérées (Communautés et Régions) de garantir le droit à la vie privée. Les Régions et Communautés sont donc compétentes pour accroître le seuil de protection de la vie privée des citoyens mais pas pour le restreindre en deçà de ce que permet le fédéral. Rappelons qu'à la fois le fédéral et les entités fédérées sont tenues par les obligations positives découlant de l'article 8 de la C.E.D.H., article qui constitue à son tour le cadre général de toute action de l'Etat belge, des Communautés ou des Régions. (3) Notons également qu'en Belgique des normes différentes protègent la vie privée, le secret de la correspondance[33] (sur lequel nous reviendrons plus bas), et l'inviolabilité du domicile[34].

électronique, *à paraître*, p. 32 et les références citées : C.A., arrêt n° 202/2004 relatif à la loi du 6 janvier 2003 concernant les méthodes particulières de recherche et quelques autres méthodes d'enquête : « *L'article 8.2 de la convention précitée qui permet une ingérence d'une autorité publique dans les droits qu'il garantit n'exige pas que cette ingérence soit prévue par une « loi » au sens formel du terme, le mot loi y signifiant toute règle de droit d'application générale et impersonnelle. Par contre, le même mot « loi » utilisé à l'article 22 de la Constitution désigne une disposition législative.* ». Concernant l'autorité législative belge compétente (Etat fédéral, Régions, Communautés) pour créer une ingérence dans la vie privée, voyez l'article précité.

[31] C.A., n° 16/2005, *op.cit.,* B.5.2

[32] C.A., n° 16/2005, *ibidem.*

[33] Article 29 de la Constitution belge stipulant que « *Le secret des lettres est inviolable.*

3. La protection de la vie privée à l'égard des traitements de données à caractère personnel

Comme mentionné plus haut, notre législation sur la protection de la vie privée à l'égard des traitements de données à caractère personnel est la transposition des directives européennes. La protection des données à caractère personnel est régie par la loi du 08 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel (LVP, ci-après). Cette législation s'applique à tout traitement de données à caractère personnel automatisé en tout ou en partie[35]. Il convient de préciser les termes employés ci-dessus afin de mieux cerner leur champ d'application (section 3.1.), avant de décrire les devoirs et droits tant du responsable que de la personne concernée (section 3.2.).

3.1. Concepts clés

1. Une donnée à caractère personnel est toute information concernant une personne physique identifiée ou identifiable. Est réputé identifiable une personne qui peut être identifiée directement ou indirectement notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale.

Sont donc des données à caractère personnel : un nom, un prénom, une date de naissance, un numéro de téléphone, une adresse postale, une adresse électronique, une adresse IP[36], un numéro de

La loi détermine quels sont les agents responsables de la violation du secret des lettres confiées à la poste. »

[34] Article 15 de la Constitution belge stipulant que « *Le domicile est inviolable; aucune visite domiciliaire ne peut avoir lieu que dans les cas prévus par la loi et dans la forme qu'elle prescrit.* »

[35] Article 3 LVP.

[36] Une adresse IP est une adresse relevant de l' « Internet protocole ». Ce protocole est le principal protocole utilisé sur Internet pour permettre à deux entités de communiquer entre elles. Chaque entité (terminal) doit donc disposer d'une adresse (d'une identité). Les adresses IP sont soit permanentes

sécurité sociale, des préférences en matière de repas voire des contre-indications en raison de certaines maladies (ex. : diabète), un login et un mot de passe, un log sur un réseau[37], une photo, une vidéo[38], des données médicales telles que le résultat d'un examen médical, une condamnation, un refus ou une autorisation émanant d'une administration, une donnée de localisation telle que la localisation géographique d'un terminal personnel (GSM, GPS), etc.

Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens susceptibles d'être raisonnablement[39] mis en œuvre, soit par le responsable du traitement, soit par une autre personne, pour identifier la dite personne[40]. En résumé, il faut et il suffit qu'une entité puisse faire le

c'est-à-dire qu'un terminal dispose de façon permanente de la même adresse IP, soit temporaires auquel cas, à chaque connexion, les fournisseurs d'accès attribuent une adresse IP. Une adresse IP est donc un identifiant unique relatif à un terminal et peut être qualifiée de donnée à caractère personnel puisque les fournisseurs d'accès peuvent faire le lien entre l'adresse IP et la personne titulaire du compte. L'adresse IP est donc une donnée relative à une personne identifiable par un tiers. Voy. sur la collecte d'adresses IP dans le cadre de la recherche d'infractions au droit d'auteur sur Internet, Commission de la protection de la vie privée, Avis d'initiative n° 44/2001 concernant la compatibilité de la recherche d'infractions au droit d'auteur commises sur Internet avec les dispositions juridiques protégeant les données à caractère personnel et les télécommunications, disponible sur www.juridat.be

[37] On entend par-là une inscription dans un log file (fichier ou plutôt journal de bord enregistrant les personnes se connectant au réseau).

[38] Considérant l'article 14 de la directive 95/46/CE stipulant que « compte tenu de l'importance du développement en cours, dans le cadre de la société de l'information, les techniques pour capter, transmettre, manipuler, enregistrer, conserver ou communiquer les données constituées par des sons et des images, relatives à des personnes physiques, la présente directive est appelée à s'appliquer aux traitements portant sur ces données.

[39] A noter que la notion de « raisonnable » est sujette à interprétation. Cependant on peut affirmer qu'il est indifférent que ce lien soit effectué par le responsable du traitement ou par un tiers. Il est également indifférent que le lien soit effectivement établi et qu'il puisse l'être. D'autre part, de par l'usage des bases de données numériques et leur interconnexion aisée, il nous semble qu'il sera rare que l'on ne puisse raisonnablement pas faire le lien entre une donnée et une personne.

[40] Considérant l'article 26 de la directive 95/46/CE et projet de loi transposant la directive 95/46/CE du 24 octobre 1995 du Parlement européen et du conseil

lien entre la personne et la donnée qui la concerne pour que la donnée soit considérée comme une donnée à caractère personnel.

Quid des données codées ou anonymes ? Les données codées sont également à considérer comme des données à caractère personnel, même lorsque le responsable du traitement lui-même ne peut vérifier à quelle personne elles se rapportent[41], lorsque l'identification peut être effectuée par une autre personne. En ce qui concerne les données anonymes, celles-ci ne perdent la qualification de données à caractère personnel que si le caractère anonyme est absolu et que plus aucun moyen raisonnablement susceptible d'être mis en œuvre ne permet de revenir en arrière pour briser l'anonymat. Les CPAS peuvent ainsi recevoir des données statistiques anonymes ou codées, par exemple des données relatives à des profils de personnes qui pourraient nécessiter un suivi particulier.

2. Un traitement est toute opération[42] ou un ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliqués à des données à caractère personnel, tels que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction de données à caractère personnel.

Ainsi, le simple fait d'héberger un site web, de stocker des messages électroniques en vue de l'envoi et/ou de la réception, de constituer une base de données à caractère personnel (par exemple des informations sur son personnel, des log-in et mots de passe de

relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et à la libre circulation de ces données, *Doc.parl.*, Ch. repr., sess. ord. 1997-1998, n°1566/1 du 20 mai 1998, p.12.

[41] Parce qu'il ne possède pas lui-même les clés d'identification qui permettent le décodage.

[42] Une seule opération est donc à considérer comme un traitement de données à caractère personnel. Ainsi, une extraction par exemple ou une consultation unique des données à caractère personnel constitue un traitement auquel s'applique la loi du 8 décembre 1992.

son personnel ou un fichier log) voire de conserver la liste des sites web visités par son personnel constituent des traitements de données à caractère personnel. On conçoit bien d'autres traitements en ce qui concerne les usagers des CPAS : la liste des bénéficiaires d'allocation, les pensionnaires des homes des CPAS, etc..

3. Le responsable du traitement est l'entité à qui la Loi sur la Protection de la vie privée (LVP) fait supporter nombre d'obligations. La LVP le définit comme *« la personne physique ou morale, l'association de fait ou l'administration publique qui, seule ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel ».*

Soulignons que lorsqu'une norme détermine les finalités d'un traitement, le responsable du traitement est alors l'entité désignée comme telle dans la loi.

Au vu de cette définition, le CPAS lui-même à travers les décisions de son conseil sera le responsable du traitement. Il lui incombe alors de respecter certains principes et certaines obligations lorsqu'il effectuera un traitement de données à caractère personnel. On distingue du responsable du traitement, le sous-traitant qui accomplit certaines missions à la demande du responsable du traitement et pour le compte de ce dernier. Celui-ci ne peut utiliser en aucune manière les données pour son propre compte. La LVP oblige le responsable à certaines précautions dans le choix de son sous-traitant et oblige à la signature d'un contrat précisant les devoirs du sous-traitant et les missions de ce dernier. Dans le cas qui nous occupe, on peut imaginer que les CPAS recourent à certains sous-traitants par exemple pour certaines fonctions de back-up, ou parce que, trop petits et incapables de disposer eux-mêmes d'un serveur, ils louent les services d'une société tierce. On ajoute le cas fréquent où les traitements du CPAS sont hébergés voire opérés par la commune. Rappelons que dans de tels cas, la commune est sous-traitante, ce qui implique que des précautions doivent être prises pour que les fichiers du CPAS et de la commune soient maintenus distincts et qu'un contrat entre le CPAS, responsable, et la commune, sous-traitante, précise bien les missions de la commune vis-à-vis des fichiers des CPAS.

3.2. Règles à respecter par les CPAS en matière de protection de la vie privée

3.2.1 Principe de transparence (droit d'information, notification à la commission de protection de la vie privée, droit d'accès/rectification)

L'information de la personne concernée du traitement la concernant est la pierre angulaire de la législation de protection des données à caractère personnel et sa raison d'être (sa ratio legis) est la suivante : la personne concernée doit être informée du traitement de données la concernant[43] afin de pouvoir exercer l'ensemble des droits que lui reconnaît la LVP et exercer ainsi *« un certain contrôle de l'exercice par le responsable du traitement du respect des prescrits légaux et de la qualité des données »*[44].

Ce droit permet ainsi à tout un chacun d'exercer son droit à l'auto-détermination informationnelle, c'est-à-dire la maîtrise de la circulation de ses données à caractère personnel, ce qui ne signifie pas nécessairement le droit de s'opposer mais en tout cas le droit de connaître la circulation de son image informationnelle. C'est pour cette raison que la LVP prévoit que le responsable du traitement doit fournir à la personne concernée auprès de laquelle il obtient les données la concernant au plus tard au moment où ces données sont obtenues :

1. le nom et l'adresse du responsable du traitement et, le cas échéant, de son représentant;
2. les finalités du traitement;
3. l'existence d'un droit de s'opposer, sur demande et gratuitement, au traitement de données à caractère personnel la concernant envisagé à des fins de marketing direct;

[43] La loi définit les informations qui doivent être communiquées à l'article 9 LVP

[44] D. DE ROY, C. de TERWANGNE, Y. POULLET, La convention européenne des droits de l'homme en filigrane de l'administration électronique, à paraître, p. 47.

4. d'autres informations supplémentaires, notamment :

   - les destinataires ou les catégories de destinataires des données,
   - le caractère obligatoire ou non de la réponse ainsi que les conséquences éventuelles d'un défaut de réponse,
   - l'existence d'un droit d'accès et de rectification des données la concernant;

D'après l'enquête 45 % des CPAS ayant un dossier informatique unique n'informent pas les personnes concernées par ces traitements, c'est-à-dire leurs usagers.

Les dernières informations portées au n°4 peuvent cependant ne pas être communiquées lorsque *« compte tenu des circonstances particulières dans lesquelles les données sont obtenues, ces informations supplémentaires ne sont pas nécessaires pour assurer à l'égard de la personne concernée un traitement loyal des données ».*

Attention, comme toute exception, cette exception doit s'interpréter restrictivement. De plus si on se réfère à la directive 95/46/CE, il faut voir le quatrièmement comme une possibilité d'étendre les informations devant être communiquées à la personne concernée en application du critère de loyauté et non comme une restriction à cette obligation d'information. Ainsi par exemple, si le traitement se déroule en partie à l'étranger, ce fait doit être révélé, au vu des risques accrus que le transfert de données présente pour la personne concernée[45].

De plus, en principe, lorsque les données n'ont pas été obtenues auprès de la personne concernée, c'est-à-dire auprès de l'usager, le responsable du traitement doit fournir une série d'autres informations à cette personne. Cependant l'article 29 de l'arrêté

[45] T. LEONARD, Y. POULLET, La protection des données à caractère personnel en pleine (r)évolution – La loi du 11 décembre 1998 transposant la directive 95/46/C.E. du 24 octobre 1995, J.T., 1999, n° 5928, p. 389.

Royal du 13 février 2001 portant exécution de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel[46] exonère les CPAS de cette obligation lorsqu'ils agissent en tant qu'autorité administrative à plusieurs conditions : être explicitement chargés, par ou en vertu de la loi, de rassembler et de coder les données à caractère personnel ; être soumis, à cet égard, à des mesures spécifiques visant à protéger la vie privée, instituées par ou en vertu de la loi ; agir en tant qu'organisation intermédiaire ». Est clairement visé ici le cas des données obtenues par les CPAS directement auprès de la BCSS.

Corollairement à ce devoir d'information, le responsable de traitement doit notifier à la Commission de la protection de la vie privée le traitement mis en place[47]. Cette notification doit-elle aussi comprendre une série de mentions obligatoires. L'objectif est à la fois de permettre à la Commission de tenir un registre mais aussi éventuellement de donner des avis d'initiative si un risque pour la vie privée des personnes fichées existe[48].

Remarquons toutefois qu'il existe des exonérations à l'obligation de déclaration à la Commission de la protection de la vie privée. En effet, l'Arrêté Royal du 13 février 2001 prévoit un certain nombre d'exceptions au principe de déclaration dans ses articles 51 à 62. Deux exceptions vont retenir plus particulièrement notre attention : les articles 61 et 62. Insistons sur le fait que même si *« un traitement se qualifie pour une exemption (d'information et/ou de notification) »,* cela n'empêche pas le responsable du traitement d'être obligé de fournir les informations reprises dans la déclaration à toute personne qui en fait la demande. De même, la Commission de la protection de la vie privée conserve son pouvoir d'exiger d'autres éléments d'information. L'intérêt du responsable du traitement d'être exempté

[46] A.R. du 13 février 2001 portant exécution de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, *M.B.*, 13 mars 2001. Attention, l'arrêté royal prévoit de nombreuses exceptions à ce devoir de déclaration en particulier si le traitement ne prévoit pas de communication vers les tiers.

[47] Article 17 LVP

[48] Article 30 LVP

de l'obligation de déclaration se trouve dès lors réduit étant donné que dans tous les cas il doit tenir les renseignements à la disposition de quiconque en fait la demande (droit d'accès / rectification). D'expérience, on s'est rendu compte qu'il y avait de toute façon un intérêt interne à effectuer l'exercice d'identifier pour chaque traitement de données les renseignements contenus dans la déclaration[49]. Cela permet de réaliser précisément en quoi consistent les ressources informationnelles dont on dispose, et cela représente un instrument de gestion de ces ressources[50].

La première exception vise à dispenser les « *autorités administratives, si le traitement est soumis à des réglementations particulières adoptées par ou en vertu de la loi et réglementant l'accès aux données traitées, ainsi que leur utilisation et leur obtention* »[51].

La deuxième exemption concerne les institutions de sécurité sociale au sens de la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque Carrefour de la Sécurité Sociale « à condition que pour ce qui concerne ces traitements, ces institutions de Sécurité Sociale satisfassent aux dispositions de la loi précitée et à ces arrêtés d'exécution »[52].

Dans les deux cas, l'exemption a pour objectif d'éviter de multiplier les formalités pour le responsable du traitement à condition qu'un autre texte oblige ce responsable au même type de formalités. *Ces deux exceptions ne suffisent cependant pas pour justifier le fait que seulement 9 % des CPAS ayant un dossier informatisé unique couvrant des applications bien au-delà des cas prévus par les exceptions citées ci-dessus ont effectué une déclaration à la Commission de la protection de la vie privée…*

[49] Tels que la base légale du traitement, les finalités du traitement, les catégories de données contenues, les catégories de destinataire, la période de conservation des données, etc.).

[50] C. de TERWANGNE, S. LOUVEAUX, Protection de la vie privée face au traitement de données à caractère personnel : le nouvel arrêté Royal, *J.T.*, 2001, p. 457 à 470 et plus particulièrement p. 463.

[51] Article 61 de l' A.R. du 13 février 2001, *op.cit.*

[52] Article 62 de l'A.R. du 13 février 2001, *op. cit.*

Par ailleurs, la personne concernée bénéficie également d'un droit d'accès/rectification[53] aux données la concernant.

Le droit d'accès[54] offre la possibilité à la personne concernée d'obtenir du responsable du traitement la confirmation que ces données sont ou non traitées, le contenu de ces données, leur origine et la logique sous-tendant le traitement. Pour exercer ce droit d'accès la personne concernée doit apporter la preuve de son identité. La demande doit être signée et datée, remise sur place ou envoyée par la poste, ou par tout moyen de télécommunication[55]. Le

[53] Indépendamment de cette législation il est intéressant de remarquer que l'article 8 CEDH « garantit, à moins que la protection d'un intérêt prédominant ne s'y oppose, l'accès de chacun aux informations éminemment personnelles qui se rapportent à soi, conservées par une autorité publique (arrêt Gaskin, Mikulik et Odièvre). Par ailleurs, de l'article 8 découle également, d'après l'enseignement de la Cour, un droit d'accès pour chacun aux données relatives à sa vie privée (arrêt Leander), englobant les données relatives à la vie professionnelle, aux relations commerciales (arrêt Amann) et aux données publiques dès lors que ces dernières sont, d'une manière systématique, recueillies et mémorisées dans des fichiers tenus par les pouvoirs publics (arrêt Rotaru) ». D. DE ROY, C. de TERWANGNE, Y. POULLET, La Convention européenne des droits de l'homme en filigrane de l'administration électronique, op.cit.

[54] Article 10 LVP : La personne concernée a le droit d'obtenir : *« 1. La confirmation que des données la concernant sont ou ne sont pas traitées, ainsi que des informations portant au moins sur les finalités du traitement, les catégories de données sur lesquelles il porte et les catégories de destinataires auxquels les données sont communiquées; 2. La communication, sous une forme intelligible, des données faisant l'objet des traitements, ainsi que de toute information disponible sur l'origine de ces données; 3. La connaissance de la logique qui sous-tend tout traitement automatisé des données la concernant, dans le cas des décisions automatisées; 4. Un avertissement de la faculté d'exercer les recours prévus aux articles 12 (droit de rectification) et 14 (action en cessation) et, éventuellement, de consulter le registre public prévu à l'article 18 ».*

[55] Cela offre la possibilité pour la personne concernée d'introduire la demande par courrier électronique pour autant que celui-ci soit signé au moyen d'une signature électronique équivalente à la signature manuscrite. Voy. loi du 20 octobre 2000 introduisant l'utilisation des moyens de communication et de la signature électronique dans la procédure judiciaire et extrajudiciaire, *M.B.*, 22 décembre 2000, et la loi du 9 juillet 2001 fixant certaines règles relatives au cadre juridique pour les signatures électroniques et les services de certification, *M.B.*, 29 septembre 2001.

responsable du traitement est tenu de répondre dans les 45 jours de la demande[56].

Si la personne concernée constate que les données la concernant sont inexactes ou incomplètes, la LVP lui offre la possibilité d'obtenir sans frais la rectification[57] de ses données. Elle peut également obtenir la suppression ou l'interdiction d'utilisation de toute donnée à caractère personnel la concernant qui, compte tenu du but du traitement, est incomplète ou non pertinente ou dont l'enregistrement, la communication ou la conservation sont interdits ou encore qui a été conservée au-delà de la période autorisée. *Ici nous constatons également le manque de connaissance de la législation par les CPAS car 74 % de ceux possédant un dossier informatique unique n'offrent pas de droit d'accès / rectification à la personne concernée parfois comble de la naïveté, pour des raisons tenant à la sensibilité des données y étant contenues.*

Au droit d'information, d'accès/rectification et à l'obligation de notification, il faut pour être complet également ajouter le droit de recours[58] et le droit de ne pas être soumis à une décision automatisée[59].

3.2.2 Principe de proportionnalité

Ce principe est transversal dans la LVP[60]. Il implique une mise en balance entre d'une part l'intérêt de la personne concernée par la protection de sa vie privée et d'autre part l'intérêt du responsable du traitement à effectuer ce traitement. L'atteinte à la vie privée de la

[56] Article 32 de l'Arrêté Royal du 13 février 2001

[57] Article 12 LVP.

[58] Voy. article 14 LVP.

[59] Article 12bis LVP : « *Une décision produisant des effets juridiques à l'égard d'une personne ou l'affectant de manière significative ne peut être prise sur le seul fondement d'un traitement automatisé de données destiné à évaluer certains aspects de sa personnalité. […].* »

[60] En effet, la *ratio legis* de la LVP est de permettre les traitements de données à condition que l'atteinte à la vie privée soit proportionnée au traitement envisagé. Les articles 4, 2°, 3°, 5°, l'article 5, l'article 16 §2, 3° sont des traductions de ce principe de proportionnalité.

personne concernée doit être proportionnée à l'intérêt du responsable du traitement d'effectuer ce traitement. En d'autres termes, la finalité du traitement doit poursuivre un intérêt supérieur à l'intérêt des personnes concernées à ce que leurs données ne soient pas traitées. L'article 5 de la LVP réalise cette mise en balance et considère certaines finalités comme proportionnées (légitimes) a priori dans les cas suivants :

- Si la personne concernée a indubitablement donné son consentement. « *Toute manifestation de volonté peut constituer un consentement. Cela implique qu'il ne doit pas nécessairement être donné par écrit et qu'il peut être implicite, sauf exception. Le consentement doit être libre, c'est-à-dire donné en dehors de toute pression. L'idée est de prévenir toute discrimination suite au choix de la personne concernée. Le consentement doit également être spécifique. Il ne peut avoir un objet général, mais doit porter sur des traitements précisément définis notamment en leurs finalités, poursuivies par des responsables déterminés. Finalement le consentement doit être informé. Le responsable du traitement doit donc transmettre à la personne concernée toute information nécessaire à l'analyse du risque particulier que représente le traitement envisagé pour ses droits et libertés. A cet égard, l'information reçue par la personne concernée au moment de la collecte semble constituer un minimum* »[61].
- Lorsque le traitement est nécessaire à l'exécution d'un contrat, auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci; ainsi par exemple, le fait d'acheter un livre sur Internet permet au vendeur de traiter mon adresse, mon numéro de carte de crédit, etc. De même si une personne âgée demande à pouvoir bénéficier des services de logement d'un home du CPAS, il va de soi que le traitement des données de cette personne est légitime pour permettre la délivrance du service par le CPAS.

[61] M.-H., BOULANGER, C. de TERWANGNE, Th. LEONARD, S. LOUVEAUX, D. MOREAU, Y. POULLET, La protection des données à caractère personnel en droit communautaire, *Telecommunications and Broadcasting Networks under EC Law : the Protection Afforded to Consumers and Undertakings in the Information Society, Köln, Bundesanzeiger,* 2000, pp. 131-183 et spécialement p.144.

- Lorsque le traitement est nécessaire au respect d'une obligation à laquelle le responsable du traitement est soumis par ou en vertu d'une loi, d'un décret ou d'une ordonnance ; ainsi un CPAS pourrait traiter des données à caractère personnel si la loi lui impose de collecter certaines informations à propos d'une aide à accorder.
- Lorsque le traitement est nécessaire à la sauvegarde de l'intérêt vital de la personne concernée;
- Lorsque le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique, dont est investi le responsable du traitement ou le tiers auquel les données sont communiquées.

Par ailleurs, ce principe signifie également que si la finalité du traitement envisagé peut être réalisée par une voie moins attentatoire à la vie privée, cette dernière doit être privilégiée.

L'objectif de ce principe gouvernant la matière est de garder un juste équilibre entre d'une part le traitement mis en place et d'autre part le respect de la vie privée. Par exemple, à propos du décret de la Communauté flamande portant publication sur Internet (sans restriction d'accès) d'une liste de sportifs ayant été contrôlés positivement à un test dopage, la Cour d'Arbitrage applique ce principe de proportionnalité lorsqu'elle écrit que *« la publication entreprise n'est pas nécessaire pour atteindre l'objectif légitime poursuivi par le législateur décrétal (empêcher les coureurs contrôlés positivement de prendre le départ d'une compétition sportive), puisque cet objectif peut également être réalisé par des moyens moins dommageables pour les intéressés»*[62] (publication sur Internet mais avec restriction d'accès ou diffusion au sein des comités organisateurs, etc.).

3.2.3 Principe de finalité du traitement

Les finalités (buts) du traitement de données à caractère personnel doivent aussi remplir certaines qualités. Elles doivent être déterminées c'est-à-dire claires, précises et fixées à priori. Ainsi, on

[62] C.A., 19 janvier 2005, n° 16/2005, point B.6.2.

ne peut concevoir une collecte de données ayant pour finalité *« une finalité laissée à la discrétion future du responsable du traitement ».*

Ces finalités doivent aussi être explicites et donc avoir une signification, un sens. Interdiction donc de prévoir des finalités obscures ne pouvant être comprises que par des experts d'un domaine particulier. Finalement elles doivent être légitimes ce qui signifient qu'elles doivent rentrer dans une des catégories prévues à l'article 5 de la LVP.

Ce principe limite également la collecte aux seules données nécessaires pour la(les) finalité(s) du traitement et interdit que les données ne soient traitées ultérieurement de manière incompatible avec cette (ces) finalité(s)[63]. La compatibilité du traitement avec la (les) finalité(s) initiales s'apprécient d'une part par rapport aux prévisions raisonnables de la personne concernée (la personne pouvait-elle prévoir cette utilisation de ses données à caractère personnel lorsqu'elle a été informée de la finalité initiale du traitement ?) et par rapport aux dispositions légales en vigueur. Serait incompatible avec la finalité initiale du traitement, par exemple, le fait d'utiliser, sans le consentement des personnes concernées[64], les données collectées dans le cadre d'une demande du droit à l'intégration sociale pour proposer à ces personnes la « vente » de biens ou services peu onéreux, ainsi les repas à domicile ou des cours d'informatique ou de conduite automobile.

3.2.4 Principe de qualité des données

Les données traitées doivent être adéquates, pertinentes et non excessives par rapport à la finalité du traitement. Concrètement, si par exemple, la finalité du traitement est l'octroi du droit à l'intégration sociale, il est interdit que les données collectées

[63] Article 4 LVP

[64] L'obtention du consentement peut être réalisée via la signature de la personne concernée au bas d'un formulaire reçu lors de la première visite au CPAS à condition que cette signature soit apposée après que due information ait été donnée sur les conséquences de celui-ci et sur les traitements qui seront opérés à partir de là.

s'étendent à des données concernant l'orientation sexuelle ou l'appartenance religieuse[65].

Les données doivent aussi être exactes, mises à jour et conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont obtenues ou pour lesquelles elles sont traitées ultérieurement. Il incombe donc au responsable du traitement de tenir à jour les données. De plus celui-ci doit limiter la durée de conservation des données au strict minimum nécessaire à la réalisation de la finalité du traitement.

3.2.5 Régime particulier pour certains types de données

Le traitement des données que l'on peut qualifier de données sensibles (données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ainsi que le traitement des données relatives a` la vie sexuelle)[66], médicales (données à caractère personnel relatives à la santé)[67] ou judiciaires (données à caractère personnel relatives à des litiges soumis aux cours et tribunaux ainsi qu'aux juridictions administratives, à des suspicions, des poursuites ou des condamnations ayant trait à des infractions, ou à des sanctions administratives ou des mesures de sûreté)[68] est en principe interdit. La LVP pose néanmoins les

[65] De plus ces données religieuses ou sexuelles sont soumises à un régime spécial : article 6 LVP.

[66] Article 6 LVP

[67] Article 7 LVP, Voy. par exemple, J.HERVEG, M.-N. VERHAEGEN, Y. POULLET, Les droits du patient face au traitement informatisé de ses données dans une finalité thérapeutique : les conditions d'une alliance entre informatique, vie privée et santé, *Revue de Droit de l'Université de Sherbrooke*, 2002, n°2, pp. 56-85.

[68] Article 8 LVP. Voy pour plus de précisions C. BURTON, Y. POULLET, A propos de l'avis de la Commission de la protection de la vie privée du 15 juin 2005 sur l'encadrement des listes noires, *R.D.T.I.*, 2005, n°23, pp. 79-122 et plus spécialement pp.110 à 114. ;M. ROOS, Données sensibles et judiciaires. Commentaires des articles 6 et 8 de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, R.B.S.S., 1993, 2/93, pp. 277 – 293.

conditions sous lesquelles un traitement de telles données est possible.

3.2.6 Sécurité des traitements

La LVP impose une série d'obligations en matière de sécurité des données personnelles. Ces obligations sont aussi bien de nature technique qu'organisationnelle. Elles consistent à prendre les mesures organisationnelles et techniques nécessaires contre, entre autres, la destruction accidentelle ou non autorisée, la perte accidentelle, la modification, l'accès et tout autre traitement non autorisé. Ces mesures doivent être élaborées en tenant compte de l'état de la technique, des frais, des risques, et de la nature des données à protéger. Il convient également de restreindre l'accès aux données et les possibilités de traitement uniquement à ce dont les personnes ont besoin pour l'exercice de leurs fonctions ou à ce qui est nécessaire pour les nécessités du service.

4. Un cas particulier de traitement de données à caractère personnel : La Banque Carrefour de la Sécurité Sociale (BCSS)

Depuis le 1 janvier 2006, les CPAS sont tenus d'intégrer le réseau de la Banque Carrefour de la Sécurité Sociale (BCSS). Cet événement majeur entraîne de nombreuses interrogations en leur sein. Cette partie a pour objectif de clarifier certains points. Dans un premier temps, l'institution et ses missions seront brièvement décrites. Ensuite, nous nous attarderons sur le procédé juridique « douteux » utilisé afin de stimuler cette connexion. Finalement, nous passerons en revue quelques obligations incombant aux CPAS de part leur intégration au sein de la BCSS.

4.1. Qu'est ce que la Banque Carrefour de la Sécurité Sociale ?

La réalisation de la Banque Carrefour de la Sécurité Sociale (BCSS) participe à ce que l'on a coutume d'appeler *« l'e-government »* ou la gouvernance électronique. Si ce terme est souvent limité aux contacts entre citoyens et administrations (« Front office »), il vise également les contacts entre les différentes administrations (« Back office »).

La BCSS est, à côté du Registre National, de la Banque Carrefour des Entreprises et d'autres en réalisation, un des ces outils qui permet de réaliser ce « back office » en créant un réseau sécurisé d'échanges de données standardisées[69]. L'objectif de ce réseau est de permettre la communication des données de manière électronique et donc de supprimer ou, du moins, diminuer l'utilisation du papier, de réduire le nombre d'erreurs d'encodage, etc..

Sans entrer dans les détails, la BCSS a plusieurs missions[70] :

- Des missions de normalisation :
  - Normalisation politique consistant à développer une stratégie commune en matière d'e-government dans le domaine de la Sécurité Sociale, à promouvoir et à veiller à l'homogénéité et à la cohérence de cette politique.. La BCSS a également pour mission de développer les projets et services qui englobent potentiellement l'ensemble des institutions de Sécurité Sociale.
  - Normalisation technique comprenant le développement des normes, des standards et de l'architecture de base nécessaires pour une mise en oeuvre efficace des TIC.
- Des missions d'assistance : La Banque Carrefour est chargée de soutenir les institutions de Sécurité Sociale afin de leur permettre, au moyen des TIC, d'exécuter d'une manière effective et efficace leurs missions au profit des utilisateurs de leurs services, avec un minimum de charges administratives et de frais pour les intéressés et, dans la mesure du possible, de leur propre initiative[71]. Elle assiste également les institutions de Sécurité Sociale lors de la mise en œuvre de la stratégie commune[72].
- Des missions de contrôle des normes techniques et de la stratégie mise en place en matière d'e-gouvernance
- Des missions de traitement de données :
  - Coordination et échange de données : La Banque Carrefour est chargée de conduire, d'organiser et d'autoriser les échanges de données sociales entre les banques de données relevant d'organismes de la sécurité sociale et en particulier de la Banque Carrefour de la Sécurité Sociale. Elle coordonne en outre les relations entre les institutions de Sécurité Sociale entre elles, d'une part, et entre ces institutions et le Registre national, d'autre part.[73]
  - Collecte de données :

[69] En effet, comme le relève la Commission de la protection de la vie, il existe trois banques de données ayant pour vocation de faciliter les flux d'informations entre administrations et services publics : le Registre national, la Banque Carrefour de la Sécurité Sociale et la Banque Carrefour des Entreprises. Avis n° 07/2002 de la Commission de la protection de la vie privée du 11 février 2002 sur le projet de loi créant une Banque Carrefour des Entreprises, disponible sur www.moniteur.be

[70] Article 2bis à 5 de la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque Carrefour de la sécurité sociale, *M.B.*, 22 février 1990, p. 03288. Pour une présentation plus complète et plus visuelle de ces missions voy. http://www.ksz-bcss.fgov.be/fr/missions/missions_1.htm#mission_1_5 . Voy. également F. ROBBEN, P. MAES, La Banque Carrefour de la Sécurité Sociale comme moteur de l'e-government du secteur social, disponible sur http://www.ksz-bcss.fgov.be/documentation/fr/documentation/Presse/La_BCSS_en_2006.pdf

[71] Article 3bis LBCSS

[72] La Banque Carrefour peut exécuter des missions en matière de gestion de l'information et de sécurité de l'information, qui lui sont confiées par le service public fédéral technologie de l'information et de la communication, Article 8bis LBCSS, cet article n'est cependant pas encore entré à vigueur à l'heure où est écrite cette contribution

[73] Article 3 LBCSS

- La BCSS tient un répertoire des personnes[74] :
- Elle collecte, enregistre et traite les données relatives à l'identification des personnes dans 3 conditions bien précises[75].
- Elle recueille des données sociales auprès des institutions de Sécurité Sociale, les enregistre, procède à leur agrégation et les communique aux personnes qui en ont besoin pour la réalisation de recherches pouvant être utiles à la connaissance, à la conception et à la gestion de la Sécurité Sociale[76].

Sur le fonctionnement de la BCSS et sans entrer dans des considérations techniques, il est intéressant de relever plusieurs éléments :

- Comme son nom l'indique, la Banque Carrefour n'est qu'un « aiguillage » (banque de données relationnelles) permettant

[74] Ce répertoire reprend, par personne, les types de données sociales à caractère personnel qui sont disponibles dans le réseau ainsi que leur localisation. Le répertoire fournit cette localisation :1° soit en mentionnant l'institution de Sécurité Sociale où ces données sont conservées; 2° soit en mentionnant la ou les branches de la Sécurité Sociale où ces données sont disponibles, lorsque une ou plusieurs institutions de Sécurité Sociale chargées de l'application de cette ou de ces branches tiennent à jour, selon les modalités fixées par le Roi, un répertoire particulier des personnes

[75] L'article 4 permet ce type de traitement dans les cas suivants :

- « pour autant que plusieurs institutions de la Sécurité Sociale aient besoin de ces données pour l'application de la Sécurité Sociale,
- pour autant que l'identification de ces personnes soit requise en exécution de la loi du 16 janvier 2003 portant création d'une Banque Carrefour des Entreprises, modernisation du registre du commerce et création de guichets d'entreprises agréés,
- ou pour autant que l'identification de ces personnes soit requise pour l'exécution des missions qui sont accordées par ou en vertu d'une loi, un décret ou une ordonnance à une autorité publique belge ou pour l'accomplissement des tâches d'intérêt général qui sont confiées par ou en vertu d'une loi, un décret ou une ordonnance à une personne physique ou à un organisme public ou privé de droit belge ».

[76] Article 5§1 LBCSS

aux informations d'être consultées par toutes les entités. On évite ainsi la multiplication des collectes de données et le risque d'erreurs y afférent. Plus précisément, elle assure des fonctions de routage, réalise des contrôles d'ordre syntaxique ainsi que des contrôles de sécurité sur différents types de communication (messages) entre les diverses institutions de Sécurité Sociale[77].

- La BCSS ne conserve pas de données « de fond » (à opposer à ce que l'on pourrait qualifier de données de référence) à l'exception du répertoire des références de la BCSS qui est composé de différentes tables : *la table des données disponibles, la table des autorisations d'accès, le répertoire des personnes*[78].
- Dans certains cas, le simple fait de savoir que tel organisme possède telles données personnelles peut suffire pour en déduire des informations. Par exemple, le fait de savoir qu'un syndicat X possède les données de Monsieur Y suffit pour révéler l'orientation politique de Monsieur Y. C'est pourquoi, il a été décidé de prévoir une centralisation en deux temps. Premier temps, un ensemble d'entités sont centralisées auprès d'une entité dite de gestion (le SPF intégration sociale dans le cas des CPAS). Dans un deuxième temps, l'entité de gestion est alors connectée à la BCSS.

Voici une illustration de l'architecture du réseau de la BCSS :

[77] Extrait de http://www.ksz-bcss.fgov.be/fr/fluxdonnees/fluxdonnees_1.htm

[78] Le table des données disponibles indique quelles données sont disponibles dans les différents types d'institutions de Sécurité Sociale selon les différents types de dossier ; la table des autorisations d'accès indiquent à quelles données chaque institution de Sécurité Sociale a accès ; le répertoire des personnes indique pour quelles personnes, en quelle quantité et pour quelle période, des institutions de Sécurité Sociale détiennent des données. Pour plus de précisions sur ces différentes tables voy. http://www.ksz-bcss.fgov.be/fr/fluxdonnees/fluxdonnees_2.htm

79

4.2. L'intégration des CPAS au sein de la BCSS : la méthode juridique utilisée et ses éventuelles faiblesses

Le 18 février 2004, une circulaire[80] émanant du ministère de l'intégration sociale et adressée aux CPAS annonçait, non sans certaines imprécisions, leur obligation de s'intégrer au sein de la BCSS. Il est intéressant de remarquer que l'intégration des CPAS au sein de la BCSS était prévue de longue date. En effet, depuis la création de la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque Carrefour de la Sécurité Sociale[81], la

[79] Extrait de http://www.ksz-bcss.fgov.be/Fr/missions/missions_3.htm

[80] Circulaire TC/EC/23.09 du 18 février 2004 concernant la connexion des CPAS a la Banque Carrefour de la Sécurité Sociale et la loi du 15 janvier 1990 relative a la création et a l'organisation de la Banque Carrefour, disponible sur http://www.mi-is.be/documents/circ_t&c_18-02.pdf

[81] Article 2bis de la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque Carrefour de la Sécurité Sociale, *M.B.*, 22 février 1990, p. 03288.

matière du droit à un minimum de moyen d'existence[82] est comprise dans le champ des applications tombant sous la compétence partielle de la BCSS.

On peut dès lors s'interroger sur la précipitation avec laquelle les CPAS ont été tenus d'intégrer le réseau pour le 1 janvier 2006 alors que cette intégration était prévue de longue date. N'aurait-il pas fallu prévoir un calendrier d'intégration plus long, une procédure d'accompagnement et une obligation de connexion retardée au 1 janvier 2007 par exemple ?

Ce « coup d'accélérateur » relève d'une politique volontariste en la matière. En effet, le Gouvernement dans sa déclaration gouvernementale de juillet 2003 mit l'intégration des CPAS au sein de la BCSS au rang des priorités. S'il est vrai que cette intégration présente en principe de nombreux avantages, on ne peut que constater avec regret le manque d'encadrement des CPAS[83] lors de leur intégration au réseau BCSS et le désordre qui régna à propos de cette intégration et ce malgré les quelques initiatives prises ça et là.

4.2.1 La double intégration des CPAS au sein de la BCSS

L'intégration des CPAS à la BCSS s'est faite en deux temps : le premier temps que l'on peut qualifier d'intégration partielle et le second, d'intégration totale.

4.2.1.1 L'intégration partielle

Elle s'est produite en février 1990 via la loi BCSS[84]. Par le jeu de dominos suivant, les CPAS se sont trouvés partiellement inclus dans le champ d'application de la BCSS : les institutions de Sécurité Sociale sont tenues de se connecter à la BCSS. Ces institutions

[82] Aujourd'hui appelé droit à l'intégration sociale.

[83] Il faut toutefois signaler la création d'une cellule de sécurité au sein du SPP IS (y compris un help-desk) et la demande du Ministre de l'intégration sociale à l'Union des Villes des Communes d'accompagner les CPAS dans cette intégration.

[84] Ci-après désignée LBCSS.

sont, entre autres, définies comme celles chargées de l'application de la Sécurité Sociale et cette dernière notion comprend d'après l'article 2, 1°, de la Loi organique de la Banque Carrefour de la Sécurité Sociale (LBCSS) : *« l'ensemble des branches du régime de l'aide sociale constitué par les allocations aux personnes handicapées, le droit à l'intégration sociale (anciennement MINIMEX, ndlr), les prestations familiales garanties, le revenu garanti aux personnes âgées et la garantie de revenus aux personnes âgées »*. Les CPAS étaient déjà compris dans la notion d'institutions sociales devant utiliser la BCSS mais uniquement pour ce qui concernait le droit à l'intégration sociale[85]. Cependant, faute d'entité de gestion pouvant centraliser la connexion de l'ensemble des CPAS, cette intégration n'eut pas lieu. Ce manque fut comblé en février 1998 et un groupe de travail fut crée pour encadrer l'intégration des CPAS au sein de la BCSS.

4.2.1.2 L'intégration totale

La LBCSS prévoit dans son article 18 la possibilité pour le Roi d'étendre le champ d'application *« à d'autres personnes que les institutions de Sécurité Sociale, tout ou partie des droits et obligations résultant de la présente loi et de ses mesures d'exécution. Ces personnes sont intégrées dans le réseau dans la mesure de l'extension décidée »*[86]. Depuis mars 2005 et grâce à

[85] Voy. dans ce sens, l'avis du Conseil d' Etat, n° 07/2004 du 14 juin 2004 sur le projet d'arrêté royal relatif à l'extension du réseau de la Sécurité Sociale aux Centres Publics d'Aide Sociale, en ce qui concerne leurs missions relatives au droit à l'aide sociale, en application de l'article 18 de la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque Carrefour de la Sécurité Sociale, Commission de la protection de la vie privée, disponible sur www.moniteur.be : « *Etant chargés de l'application de la Sécurité Sociale, plus précisément de la réglementation relative au droit à l'intégration sociale, les Centres Publics d'Aide Sociale sont à ce titre considérés comme des institutions de sécurité sociale et font déjà partie comme tels du réseau de la sécurité sociale.* »

[86] Cet article stipule qu' *« Aux conditions et selon les modalités qu'Il fixe, le Roi peut, par arrêté délibéré en Conseil des Ministres, sur proposition du Comité de gestion de la Banque-carrefour et après avis de la Commission de la protection de la vie privée (...), étendre à d'autres personnes que les institutions de sécurité sociale, tout ou partie des droits et obligations résultant de la présente loi et de ses mesures d'exécution. Ces personnes sont intégrées dans le réseau dans la mesure de l'extension décidée. »*

cette délégation au Roi, les CPAS sont assimilés à des institutions de sécurité sociale et les données qu'ils traitent sont assimilées à des données sociales. Cette assimilation est cependant doublement limitée car elle ne vise que ce qui concerne l'exécution des missions d'aide sociale et l'Arrêté Royal[87] d'extension ne vise qu'un certain nombre d'articles de la loi du 15 janvier 1990 relative à la BCSS.

Si on compare les deux procédés utilisés, on constate que d'une part les CPAS sont censés faire partie de la BCSS depuis 1990 mais uniquement en ce qui concerne le droit à l'intégration sociale et que d'autre part, ils sont inclus dans le champ d'application de la LBCSS depuis janvier 2005 pour l'entièreté de leurs missions relevant de l'aide sociale (en ce compris le droit à l'intégration sociale).

4.2.2 Sur l'obligation de demander les subsides via la BCSS

Si l'objectif de connecter les CPAS à la BCSS est louable et souhaitable, il est permis de s'inquiéter quant aux procédés

[87] A.R. du 4 mars 2005 relatif à l'extension du réseau de la sécurité sociale aux centres publiques d'aide sociale, en ce qui concerne leurs missions relatives au droit à l'aide sociale, en application de l'article 18 de la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-carrefour de la Sécurité sociale, *M.B.*, 31 mars 2005, p. 13898. L'article 1 stipule que *« § 1er. Les articles 6, 8, 9, 10 à 17, 20, 22 à 26, 28, 34, 46 à 48 et 53 à 71 de la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-carrefour de la Sécurité sociale, et les arrêtés pris en exécution de ces articles, s'appliquent aux centres publics d'aide sociale, pour autant qu'ils soient chargés de l'exécution de missions relatives au droit à l'aide sociale.*

§ 2. Pour l'application du § 1er :

1° les centres publics d'aide sociale sont assimilés à des institutions de sécurité sociale;

2° les données traitées par les centres publics d'aide sociale en vue de l'exécution de leurs missions relatives droit à l'aide sociale sont assimilées à des données sociales;

3° l'exécution de missions relatives au droit à l'aide sociale est assimilée à l'application de la sécurité sociale. »

juridiques utilisés pour « stimuler » cette connexion. Par circulaire, le Ministre de l'Intégration sociale impose aux CPAS d'utiliser la BCSS *« pour le transfert des données concernant la demande de la subvention de l'Etat, dans le cadre de la **loi relative au droit à l'intégration sociale** »*[88] (Nous soulignons).

S'il n'appartient pas à l'auteur de se prononcer sur l'opportunité d'un tel procédé, on peut toutefois s'interroger sur la légalité de celui-ci. En effet, la matière du droit à l'intégration sociale est régie par la loi concernant le droit à l'intégration sociale[89]. Cette loi en son article 44 prévoit que *« le Roi détermine, par arrêté délibéré en Conseil des Ministres, les conditions et les modalités relatives au paiement des subventions ainsi qu'au paiement d'avances ».*

LBCSS	***Loi intégration sociale***
Article 18 : Délégation au Roi pour étendre le champ d'application de la LBCSS	Article 44 : Délégation au Roi pour déterminer les conditions et modalités relatives au paiement des subventions
AR du 04 mars 2005 : Article 2 prévoit une délégation aux ministres compétents pour l'exécution du présent AR : *« Notre Ministre de l'Intérieur, Notre Ministre des Affaires sociales et de la Santé publique, Notre Ministre des Classes moyennes et de l'Agriculture, Notre Ministre de l'Emploi, Notre Ministre de l'Intégration sociale et Notre Ministre des Pensions sont chargés, chacun en ce qui le concerne, de l'exécution du présent arrêté. »*[90]	Pas d'AR

[88] Circulaire du 01 février 2005 concernant l'intégration des CPAS dans le réseau de la Sécurité sociale, disponible sur http://www.mi-is.be

[89] L. du 26 mai 2002 concernant le droit à l'intégration sociale, *M.B.*, 31 juillet 2002, p. 33610.

[90] Nous soulignons .

LBCSS	***Loi intégration sociale***
Circulaires du Ministre de l'Intégration Sociale imposant aux CPAS d'utiliser la BCSS	/

Se pose dès lors la question suivante : pourrait-on considérer que les différentes circulaires prises par le Ministre de l'Intégration sociale permettent de couvrir les exigences de l'article 44 de la loi concernant le droit à l'intégration sociale ?

Ne pourrait-on pas trouver dans l'article 2 de l'Arrêté Royal du 4 mars 2005[91] une délégation aux Ministres compétents permettant de satisfaire les exigences de l'article 44 de la loi concernant le droit à l'intégration sociale[92] ? Formulée autrement la question est la suivante : les modalités relatives au paiement des subventions font-elles partie ou non des compétences déléguées au Ministre de l'intégration sociale via l'article 2 de l'Arrêté Royal du 04 mars 2005 ?

Afin de répondre à cette question il convient de délimiter le champ d'application des différentes dispositions.

La loi concernant le droit à l'intégration sociale vise à réglementer les conditions d'octroi du droit à l'intégration sociale, ses bénéficiaires, la procédure à suivre. Elle vise également, et cela est d'importance pour notre matière, à régler la question de la subvention de l'Etat.

La loi sur la BCSS vise quant à elle l'instauration de la BCSS, son fonctionnement, et des mesures de sécurité. Nous sommes bien en présence de deux lois générales dont les champs d'application sont différents. Nous ne voyons donc pas comment un AR ou une circulaire ministérielle prise sur base d'une délégation prévue par la loi BCSS pourrait se substituer à un AR devant être pris sur base de la loi concernant le droit à l'intégration sociale.

[91] Arrêté étendant le champ d'application de la LBCSS aux CPAS, voy. note 19.

[92] En effet, cet AR a été délibéré en Conseil des Ministres et a reçu un avis positif du Conseil d'Etat.

Mais imaginons que la délégation au Ministre compétent présente dans l'AR du 04 mars 2005[93] contienne via les dispositions citées à l'article 1 de cet AR une délégation pour la matière qui nous concerne.

Pourrait-on alors substituer une circulaire à un arrêté royal délibéré en Conseil des Ministres ? En principe non ! Cependant une circulaire peut couvrir un acte réglementaire. Mais si tel est le cas, elle doit alors *« répondre à l'ensemble des conditions de légalité externe et interne des actes administratifs unilatéraux »*[94].

A ce titre, les « circulaires – actes réglementaires » dont il est question *in casu* présentent deux vices de forme : l'absence de délibération en Conseil des Ministres[95] et l'absence d'avis du Conseil d'Etat[96]. En effet, ni l'un ni l'autre n'ont été accomplis dans le cas d'espèce. L'obligation d'effectuer les demandes de subvention concernant le droit à l'intégration sociale uniquement via la BCSS est donc une obligation contestable du point de vue de la légalité formelle. Il semblerait donc que cette obligation de demande de subvention concernant le droit à l'intégration sociale via la BCSS n'ait aucune base légale valable. Pour couvrir cette irrégularité, il suffirait cependant qu'un AR soit pris sur base de l'article 44 de la loi concernant le droit à l'intégration sociale.

En l'absence d'un tel Arrêté Royal, si un CPAS n'effectue pas une demande de subvention via la BCSS comme exigé par les circulaires du Ministre de l'Intégration sociale et que celles-ci lui sont refusées, quelles seront ses possibilités de recours ?

Un CPAS qui se verrait opposer un refus aux demandes de subventions au motif qu'elles n'ont pas été effectuées via la BCSS,

[93] Voy. *Supra,* note 14

[94] P. LEWALLE, *Contentieux administratif*, Collection de la faculté de droit de l'Université de Liège, Larcier, 2° édition, 2002, p. 852, n°469.

[95] Voy. par exemple, C.E., 27 juin 1972, *A.S.B.L. Fédération royale des associations d'ingénieurs et autres c. Etat belge*, n° 15434, Rec., p. 493.

[96] En effet, l'article 3 des lois coordonnées du 12 janvier 1973 sur le Conseil d'Etat « oblige les ministres à soumettre à l'avis de la section législation tous les projets d'arrêtés réglementaires, hors les cas d'urgence spécialement motivés.»

pourrait attaquer l'Etat Belge devant les Cours et Tribunaux de l'ordre judiciaire afin d'obtenir cette subvention. Fort à parier que le Ministre leur opposera la circulaire. Il suffira alors au CPAS demandeur d'opposer l'exception d'illégalité prévue à l'article 159 de la Constitution[97].

D'un point de vue moins légaliste, on pourrait s'inquiéter de l'importance[98] des subventions perçues par les CPAS suite à l'octroi de droits à l'intégration sociale et de la survie des CPAS s'ils n'arrivent pas « à accrocher » le wagon BCSS. En effet, les dépenses engendrées par cette mission représentent en moyenne 17,4 %[99] des dépenses d'un CPAS. Si celui-ci ne peut récupérer cet argent faute d'utiliser la BCSS, il est tout à fait possible qu'il soit dans l'impossibilité matérielle d'exercer sinon la totalité de sa mission du moins celle relative au versement des droits à l'intégration sociale.

Or la Constitution garantit les droits économiques, sociaux et culturels et particulièrement le droit à l'aide sociale, notion englobant le droit au revenu d'intégration sociale. Qu'adviendra-t-il de ce droit constitutionnel si les CPAS ne se chargent plus, faute de moyens, de ce volet de l'aide sociale ?

4.3. Quelques conséquences juridiques de cette intégration

L'intégration des CPAS entraîne l'application d'une série de dispositions. Ces dispositions comprennent différentes obligations sanctionnées pénalement. C'est pourquoi, nous passerons en revue les obligations incombant aux CPAS du fait de leur connexion à la BCSS en les regroupant par catégories.

[97] « *Les cours et tribunaux n'appliqueront les arrêtés et règlements généraux, provinciaux et locaux, qu'autant qu'ils seront conformes aux lois* », Constitution Belge, article 159.

[98] Sur cette question, voy. l'analyse financière de Dexia présentée aux CPAS lors de l'Assemblée générale du 9 décembre 2005, disponible sur http://www.uvcw.be/espaces/cpas

[99] *Ibidem.*

4.3.1 Quelles sont les obligations incombant aux CPAS en ce qui concerne les données sociales[100] ?

De manière non exhaustive, citons :

4.3.1.1 Des obligations d'enregistrement et de communication des données :

- Dans les cas où la BCSS a réparti les tâches d'enregistrement de manière fonctionnelle, les institutions de sécurité sociale sont tenues d'enregistrer les données de leurs usagers sociaux dans leurs bases de données et de les mettre à jour[101].

- Ensuite, deux obligations complémentaires existent. Les CPAS ont l'obligation de communiquer toutes les données nécessaires à la BCSS pour accomplir leur mission et corollairement, les CPAS sont tenus de les demander exclusivement à la BCSS[102] sauf pour les cas où ils sont eux-mêmes responsables de l'enregistrement de ces données[103]. Par exemple, dans le cas où les CPAS possèdent déjà un accès au Registre National via une ligne directe en émulation de terminal, ils seront tenus de ne plus user de celle-ci et d'utiliser la BCSS.

4.3.1.2 Des obligations découlant du traitement de données :

Comme mentionné plus haut[104], une donnée sociale est quasiment toujours une donnée à caractère personnel. Par conséquent la

[100] Cette notion est définie à l'article 2, 4° de la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque Carrefour de la Sécurité Sociale, *op.cit.* Sur un plan théorique, nous nous interrogeons sur l'utilité de la distinction entre les données sociales et les données sociales à caractère personnel. En effet, on voit mal comment une donnée utilisée par la BCSS pourrait ne pas être liée à une personne identifiée ou identifiable et donc être une donnée à caractère personnel.

[101] Art. 9 LBCSS

[102] Art. 10 et 11 LBCSS

[103] Art. 12 LBCSS

[104] Voy. note de bas de page 32.

législation de protection des données à caractère personnel a vocation de s'appliquer aux traitements effectués par les CPAS via la BCSS.

Mais quel est le rapport entre ces deux normes ? Nous sommes d'avis que la LBCSS est à considérer comme une lex specialis vis-à-vis de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel pour ce qui concerne les dispositions ayant trait aux données à caractère personnel.

Par conséquent,

- si la LBCSS règle spécifiquement une question, cette disposition s'imposera et les dispositions de la LVP contradictoire s'écarteront en vertu du principe général « lex specialis derogat generali »[105], à condition que l'application de la loi BCSS ne prive pas la personne concernée d'un droit fondamental accordé par la LVP à la personne concernée..
- si la LBCSS se réfère explicitement à la LVP, il faudra alors appliquer cette dernière[106].
- si la LBCSS n'aborde pas un point de droit, il faudra se référer à la loi générale. Par exemple, concernant le rapport entre chaque CPAS et ses bénéficiaires, il faudra se référer à la LVP.
- si la loi spécifique a abordé un point de droit mais de manière partielle, il faudra se référer à la LVP pour éventuellement compléter ses dispositions.[107]

[105] Voy. par exemple, les articles 14, 15, 20 §2 et 43 alinéa 3 LBCSS.

[106] Voy. par exemple l'article 5§3 LBCSS.

[107] Voy. par exemple les article 22 et 23 LBCSS.

4.3.1.3 Des obligations de sécurité complexes mais d'importance primordiale[108] :

Pourquoi prévoir tant de mesures de sécurité ?

Par le passé, les données à caractère personnel et/ou données sociales bénéficiaient d'une protection simplement via leur support - le support papier. A l'heure du « tout numérique » et de la généralisation des réseaux, cette protection de fait tend à disparaître. Dans des écrits précédents, un des auteurs du présent texte identifie quatre grandes catégories de risques auxquels la législation de protection des données à caractère personnel tente de donner une réponse satisfaisante : les risques de perte de contrôle, de réutilisation des données, de manque de proportionnalité et d'inexactitude des données[109]. La législation sur la BCSS envisage plus particulièrement certaines questions.

Mais afin de mieux cerner les risques que représentent les traitements de données, prenons quelques exemples… Si par le passé, copier un certain nombre de données demandait un temps certain, aujourd'hui cela ne nécessite que quelques clics et quelques secondes. Là où il y a quelques années, pour pouvoir «voler » un nombre important de données, il fallait franchir physiquement des enceintes, s'équiper d'un véhicule de transport, de nombreuses personnes pour transporter les dossiers, aujourd'hui, il suffit de

[108] Voy. dans ce sens, l'avis n° 07/2004 du 14 juin 2004 sur le projet d'arrêté royal relatif à l'extension du réseau de la sécurité sociale aux centres publics d'aide sociale, en ce qui concerne leurs missions relatives au droit à l'aide sociale, en application de l'article 18 de la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque Carrefour de la Sécurité Sociale, Commission de la protection de la vie privée, disponible sur www.moniteur.be : « La Commission fait remarquer que le projet d'arrêté royal a pour conséquence que les centres publics d'aide sociale sont soumis à certaines obligations spécifiques sur le plan de la sécurité de l'information, en particulier l'obligation de désigner en leur sein un conseiller en sécurité, conformément aux articles 17, 24 et 25 de la loi du 15 janvier 1990 et à l'arrêté royal du 12 août 1993 relatif à l'organisation de la sécurité de l'information dans les institutions de sécurité sociale. »

[109] Cf. notamment, POULLET Y., « Protection des données à caractère personnel et obligation de sécurité », in *La sécurité informatique entre technique et droit,* Bruxelles, Story scientia*,* 1998, *pp.* 195-224.

pénétrer sur un terminal informatique ayant accès au réseau et de les copier sur un support numérique tel que un CD, DVD ou autres… En effet, tout terminal connecté à la BCSS offre potentiellement un accès à l'ensemble des données sociales de la population y compris le registre national. Là où il aurait fallu qu'un vol ait lieu dans chaque commune belge, il ne suffit aujourd'hui que d'un accès à un terminal…

Afin de déterminer les mesures de sécurité devant être mises en place, il convient de prendre en compte une série d'articles provenant de législations différentes. On cite les articles 17 et 22 à 25 de la loi BCSS, l'Arrêté Royal du 12 août 1993 relatif à l'organisation de la sécurité de l'information dans les institutions de Sécurité Sociale[110] et surtout l'article 16 de la loi vie privée[111].

Une obligation de conservation parfaite des données (Article 22 LBCSS)

L'article 22 de la LBCSS stipule que « *La Banque Carrefour et les institutions de sécurité sociale sont tenues de prendre toutes les mesures qui permettent de garantir la parfaite conservation des données sociales à caractère personnel* ».

Mais que faut-il entendre par « parfaite conservation » des données ? Il convient de lire cet article à la lumière de l'article 16 de la LVP. Par conséquent, on peut sans risque affirmer que cette obligation vise plus précisément à ce que le responsable du traitement, c'est à dire le CPAS, fasse *« toute diligence pour tenir les données à jour, pour rectifier ou supprimer les données inexactes, incomplètes, ou non pertinentes ».* Il doit par ailleurs prendre les mesures techniques et organisationnelles requises pour protéger les données à caractère personnel contre la destruction accidentelle ou non autorisée, contre la perte accidentelle ainsi que contre la modification, l'accès et tout autre traitement non autorisé de données à caractère personnel. Ces mesures doivent assurer un niveau de protection adéquat, compte tenu, d'une part, de l'état de la

[110] A.R. du 12 août 1993 relatif à l'organisation de la sécurité de l'information dans les institutions de sécurité sociale, M.B., 21 août 1993, p. 18487.

[111] L. du 08 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, *M.B.*, 18 mars 1993, p. 05801.

technique en la matière et des frais qu'entraîne l'application de ces mesures et, d'autre part, de la nature des données à protéger et des risques potentiels. Si une sécurité absolue n'est donc pas requise, le mot « *parfaite* » indique qu'en l'occurrence, les CPAS au vu des données sensibles qu'ils traitent et des risques que les personnes concernées pourraient encourir suite à la divulgation des données doivent mettre la barre de la sécurité très haut[112].

Dans l'hypothèse où ces obligations ne seraient pas respectées par les CPAS, ceux-ci risquent d'encourir des amendes de cent à deux mille francs[113].

La mise en place d'une politique d'accès aux données (Article 23 LBCSS)

Cet article stipule que *« les personnes qui interviennent dans l'application de la sécurité sociale ne peuvent obtenir communication que des données sociales à caractère personnel dont elles ont besoin pour cette application. Lorsque ces personnes ont reçu communication de données sociales à caractère personnel, elles ne peuvent en disposer que le temps nécessaire pour l'application de la sécurité sociale et elles sont tenues de prendre les mesures qui permettent d'en garantir le caractère confidentiel ainsi que l'usage aux seules fins prévues par ou en vertu de la présente loi ou pour l'application de leurs obligations légales. ».*

La LVP quant à elle, stipule que les responsables du traitement doivent *« veiller à ce que, pour les personnes agissant sous son autorité, l'accès aux données et les possibilités de traitement soient limités à ce dont ces personnes ont besoin pour l'exercice de leurs fonctions ou à ce qui est nécessaire pour les nécessités du service »*[114].

[112] Rappelons que l'obligation de sécurité vise à la fois l'intégrité des données (pas de modification des données), la confidentialité des données (pas d'accès pour des personnes non autorisées) et leur disponibilité (garantie que les données seront accessibles et traitables aux moments prévus et par les personnes autorisées)

[113] Article 61, 3° LBCSS et article 38 de la loi vie privée. A convertir en euros et à multiplier par 200. Les amendes prévues sont, par conséquent, de 500€ à 10 000€

[114] Article 16§2, 1° loi vie privée

L'idée sous-jacente à ces dispositions est la suivante : les données à caractère personnel doivent être utilisées uniquement quand c'est nécessaire et par les seules personnes autorisées à les utiliser. Ces obligations concernent aussi bien le nombre de données que la durée de leur usage. En cas de violation de ces dispositions, les CPAS risquent de se voir condamnés à une amende de cent à deux mille francs[115].

L'instauration d'un conseiller en sécurité (Article 17, 24, 25 LBCSS)

Comme nous l'avons vu plus haut, la sécurité du réseau de la BCSS est primordiale. Cette sécurité passe également par l'instauration dans chaque institution de sécurité sociale d'un service chargé de la sécurité ou du moins d'un conseiller en sécurité. Ceci est d'ailleurs imposé par l'article 24 de la LBCSS. La question des conseillers en sécurité est une des préoccupations majeures des CPAS. En effet, en plus de demander des compétences pointues en informatique, elle impose une surcharge de travail aux CPAS et donc de nouveaux coûts. Heureusement, cette question a fait l'objet de notes ou avis explicatifs[116].

A) Qui peut être conseiller en sécurité?

Quiconque disposant d'une connaissance suffisante de la structure informatique de l'institution ainsi que de la sécurité de l'information. Cette personne doit en outre tenir en permanence cette connaissance à jour[117].

[115] Article 61, 4° LBCSS. A convertir en euros et à multiplier par 200. Les amendes prévues sont par conséquent de 500€ à 10 000€.

[116] Nous pouvons citer à titre non exhaustif : Avis n°99/09 du comité sectoriel de la sécurité sociale du 09 novembre 1999 modifié le 25 juillet 2000 relatif à diverses questions posées par le Ministre des affaires sociales, de la santé publique et de l'environnement concernant les conseillers en sécurité des centres publics d'aide sociale, disponible sur http://www.mi-is.be ;

[117] Article 6 de l'AR du 12 août 1993 relatif à l'organisation de la sécurité de l'information dans les institutions de sécurité sociale, M.B., 21 août 1993, p. 18487.

B) Y a-t-il des incompatibilités entre cette fonction et d'autres ?

L'article 4 de l'AR prévoit qu'il faut éviter les incompatibilités. Cependant celles-ci ne sont pas énumérées. La logique nous amène à penser que peut être désigné conseiller en sécurité une personne autre que la personne chargée de la gestion journalière de l'informatique. En effet, on voit mal comment une même personne pourrait être à la fois le contrôleur et le contrôlé. Il en va de même à propos de la compatibilité entre la fonction de secrétaire de CPAS et de conseiller en sécurité[118]. Cette double fonction obligerait les personnes à une forme de *« schizophrénie »* consistant à, par exemple, s'auto informer d'une faille dans le système informatique. Le conseiller en sécurité devra idéalement être une personne n'ayant ni de fonctions dirigeantes au sein de CPAS, ni de fonction que l'on pourrait qualifier de *« gestion de l'informatique »*.

Nous conseillons donc que le conseiller en sécurité n'ait qu'une seule fonction, celle de surveiller l'application de la loi de protection des données et les prescrits entourant l'utilisation des ressources de la BCSS. Il est cependant compréhensible que cette nouvelle fonction pose des problèmes de coûts auxquels les *« petits CPAS »* ne peuvent répondre. Mais il existe certaines solutions pour ces entités : la mutualisation des conseillers en sécurité ou le recours à un service de sécurité spécialisé de l'information[119]. La seule limite à cette mutualisation est que les conseillers *« disposent d'une connaissance suffisante et du temps nécessaire pour pouvoir mener cette mission à bien »*[120].

[118] Cependant d'après l'avis n° 99/09 du comité sectoriel (cité supra), cette incompatibilité entre les fonctions de secrétaire de CPAS et de conseiller en sécurité peut cependant être levée dans les cas exceptionnels, notamment pour les CPAS de petite taille dont le personnel occupé est réduit et ne permet pas l'attribution de la fonction de conseiller en sécurité à une autre personne que le secrétaire de CPAS lui-même. Dans ce cas, celui-ci assumera toutes les fonctions imparties à la fonction de conseiller en sécurité et s'en réfèrera au Président du CPAS ainsi qu'au Conseil de l'Aide sociale le cas échéant.

[119] Article 2, al 2 et articles 11 à 13 bis de l'AR du 12 août 1993 relatif à l'organisation de la sécurité de l'information dans les institutions de sécurité sociale, op. cit.

[120] Article 4 AR

D'après notre enquête, 35% des conseillers en sécurité désignés par les CPAS sont des responsables informatiques, 34% des secrétaires de CPAS, 17% des autres membres du personnel des CPAS et 10% des autres membres du personnel communal. Dans 3% des cas il y a une mutualisation des conseillers en sécurité et dans 3%, le conseiller en sécurité désigné par les CPAS correspond à un autre personnel[121]*…*

C) Qui vérifie qu'il possède les compétences requises ?

La vérification des compétences du conseiller en sécurité des CPAS incombe aux CPAS eux-mêmes. En effet, un avis n'est émis par le comité sectoriel de la sécurité sociale que pour les conseillers présents dans les institutions gérant un réseau secondaire (par exemple : l'ONEM, l'INAMI, etc.) et non dans les institutions n'appartenant pas à un réseau secondaire comme les CPAS. Cependant, en vertu de l'article 24 de la LBCSS, l'identité du conseiller est communiquée à la BCSS et au comité sectoriel de la sécurité sociale. Ce comité est chargé de veiller au respect de la LBCSS et de ses mesures d'exécution y compris celles concernant le conseiller en sécurité et exerce donc un contrôle indirect. Pratiquement, cette communication de l'identité du conseiller en sécurité devra être faite au Ministère de l'Intégration sociale (institution de gestion) qui transmettra au comité sectoriel.

D) Que risque un CPAS s'il ne désigne pas un conseiller en sécurité ?

Conformément à l'article 62, 5° de la LBCSS, les CPAS, leurs préposés ou mandataires qui n'auront pas désigné, au sein de leur personnel ou non, selon le cas, un conseiller en sécurité seront punis d'un emprisonnement de huit jours à six mois et d'une amende de cent à cinq mille euros, ou d'une de ces peines seulement. A notre avis, la sanction serait la même s'il fallait constater que le conseiller désigné était manifestement incompétent ou ne disposait pas de l'indépendance requise.

[121] Ces chiffres sont basés sur le nombre de réponses reçues à cette question qui est de 72 CPAS.

4.4. Pour conclure sur l'intégration des CPAS dans le réseau de la Banque Carrefour de la Sécurité Sociale.

La BCSS joue un rôle central en matière de sécurité sociale au sens le plus large du terme. Elle est appelée à accroître son champ d'action à l'ensemble des institutions qui jouent un rôle en la matière. Cependant son élargissement est parfois source de problèmes pour les entités trop souvent pas ou peu préparées à intégrer le réseau de la BCSSS. On peut regretter que l'accent soit souvent mis sur les avantages de cette « banque de données » et que les obligations de sécurité et de protection des données à caractère personnel soient parfois reléguées au second plan.

Qu'en est-il des CPAS de Wallonie ? Dans notre enquête, les plus gros avantages perçus par les CPAS sur leur connexion à la Banque Carrefour de la Sécurité Sociale sont de rendre les traitements plus rapides (50% des CPAS), mais aussi de permettre un meilleur contrôle des aides octroyées aux bénéficiaires (45% des CPAS). Deux inconvénients de leur intégration perçus par ceux-ci sont une intégration lourde à mettre en place pour 39% des CPAS (procédures, démarches, normes de sécurité), mais aussi les coûts entraînés par une telle intégration à ce système (28% des CPAS)[122]. Notre objectif n'est pas de critiquer inopinément une intégration prometteuse telle que la connexion à la BCSS mais de soumettre, à la réflexion de tous, la méthode utilisée pour imposer cette connexion aux CPAS. Il va de soin que la réalisation de l'e-government est un objectif ambitieux et prometteur dont la création doit parfois s'accompagner d'impulsions fortes des pouvoirs politiques. Toutefois, cet ambitieux projet doit, pour atteindre ses objectifs, inclure l'ensemble des acteurs concernés dans l'élaboration de leur futur. Force est de constater que cela n'est actuellement pas toujours le cas et n'a pas été le cas vis-à-vis des CPAS dont on peut par ailleurs déplorer le manque de coordination

[122] Pour consulter le détail des résultats des avantages et des inconvénients de l'intégration à la Banque Carrefour de la Sécurité Sociale tels que les perçoivent les CPAS, nous vous renvoyons au rapport des résultats de notre enquête : C. BURTON, V. LAURENT, C. LOBET-MARIS, F. NAVARRE, Y. POULLET, « L'informatisation des CPAS, une informatique plurielle au service de l'action sociale », Avril 2006, Herbeumont, disponible gratuitement sur http://www.fundp.ac.be/pdf/publications/57376.pdf

et l'absence de représentation directe. Evitons une informatique subie et puisse l'informatique être négociée par les acteurs concernés.

Section II
Le secret des lettres et des communications électroniques

Les CPAS utilisent aujourd'hui de plus en plus fréquemment le courrier électronique pour dialoguer entre eux ou répondre à des demandes de leurs usagers, ou encore en vue d'effectuer des démarches administratives ou d'obtenir des subventions en provenance de différents organismes. Il est clair que cette correspondance doit être protégée. Dans quelle mesure, la protection du secret des lettres s'étend-elle au courrier électronique ?

Alors que la CEDH inclut la protection de la correspondance dans la vie privée, notre Constitution lui consacre une disposition particulière. En effet, l'article 29 de la Constitution stipule que « le secret des lettres est inviolable ». Mais cette disposition s'applique-t-elle aux courriers électroniques ?

La Cour d'appel de Liège a répondu par la négative à cette question. En effet, elle considère que *« les envois par courriels ne sont pas protégés par le secret de la correspondance, mais sont assimilés à des communications électroniques compte tenu de leur mode de transmission »*[123]. Le secret des lettres et le secret des communications électroniques sont donc deux notions distinctes, la première ne pouvant recevoir une interprétation extensive et ne couvrant pas les courriers électroniques.

En ce qui concerne le régime légal applicable en Belgique, les communications électroniques sont protégées à deux niveaux. Certaines dispositions protègent ce que l'on peut qualifier de « contenu » des communications électroniques alors que d'autres protègent le « contenant » des communications électroniques. Ce que nous qualifions de « contenant » des communications électroniques comprend les données relatives aux communications

[123] C. Trav. Liège, 23 mars 2004, R.R.D., 2004, liv. 110, p.73.

électroniques[124] telles que le nom du destinataire ou de l'expéditeur, la date d'envoi, la taille du message, le protocole utilisé, etc. Nous allons examiner en détail ces différentes dispositions.

Le contenu des communications électroniques est tout d'abord protégé par les articles 259bis et 314bis du code pénal. Les deux articles sont identiques, excepté quant aux personnes auxquelles ils s'appliquent : l'article 259bis vise les fonctionnaires et prévoit de part leur fonction des peines plus lourdes en cas d'infraction alors que l'article 314bis vise lui le reste de la population. Ces articles punissent la personne ou le fonctionnaire qui *« intentionnellement, à l'aide d'un appareil quelconque, écoute ou fait écouter, prend connaissance ou fait prendre connaissance, enregistre ou fait enregistrer, pendant leur transmission, des communications ou des télécommunications privées, auxquelles il ne prend pas part, sans le consentement de tous les participants à ces communications ou télécommunications ».*

Plusieurs commentaires sont à formuler à propos de cet article.

- Premièrement, un élément moral : *« intentionnellement »* est requis. La personne qui intercepterait le contenu de communications électroniques involontairement ne pourrait donc se voir sanctionner sur base d'un de ces articles.
- Deuxièmement, l'article ne s'applique qu'aux communications privées c'est à dire aux communications qui ne sont pas destinées à être lues par tout un chacun peu importe qu'elles soient personnelles, professionnelles ou commerciales.[125]

[124] Ces données comprennent les données de localisation (Art. 2, 7° loi du 13 juin 2005 relative aux communications électroniques : toute donnée traitée dans un réseau de communications électroniques indiquant la position géographique de l'équipement terminal d'un utilisateur final d'un service de communications électroniques accessible au public) et les données de trafic (Art. 2, 6° loi du 13 juin 2005 relative aux communications électroniques : toute donnée traitée en vue de l'acheminement d'une communication par un réseau de communications électroniques ou de la facturation de ce type de communication).

[125] TH. VERBIEST, E. WERY, *Le droit de la société de l'information. Droit européen, belge et français, Bruxelles*, Larcier, 2001, p. 188.

- Troisièmement, il faut que l'acte fautif ait lieu pendant la transmission. Une fois la transmission effectuée, l'article ne s'applique plus. Afin de mieux cerner la notion de « transmission » prenons un exemple concret[126]. Un courriel rédigé par un membre du CPAS à destination d'un bénéficiaire d'aide sociale. Le courrier électronique va d'abord être écrit sur l'ordinateur de l'expéditeur. Ensuite, une fois la rédaction terminée, il sera envoyé sur un serveur (SMTP) d'envoi. De ce serveur, le message sera dirigé vers la boîte virtuelle électronique du destinataire du message (serveur POP). Le destinataire pourra alors lorsqu'il consultera sa boîte télécharger le courriel. La doctrine est unanime pour considérer que la transmission commence au moment où le message « part » de l'ordinateur de l'expéditeur et qu'elle s'étend au minimum jusqu'à son arrivée sur la boîte virtuelle du destinataire[127]. Par contre, une partie de la doctrine[128] à laquelle nous nous rallions considère qu'elle s'étend jusqu'au moment où le destinataire du message télécharge effectivement le courriel sur son ordinateur[129].
- Quatrièmement, la personne qui intercepte la communication ne doit pas prendre part à la communication. Par conséquent, si j'enregistre le contenu d'une communication électronique à

[126] L'exemple choisi est le cas d'une personne utilisant une messagerie électronique et un serveur POP. Le raisonnement pourrait être différent si la personne utilise un système de courriel de type webmail (hotmail, yahoo, gmail). Cependant dans tous les cas la transmission ira jusqu'au serveur du destinataire.

[127] Voy. par exemple DE ROY, D., K. ROSIER, Publicité et transparence des marchés publics dématérialisés, *C.D.P.K.*, 2005, n° 1, p. 122, point 22.

[128] P. DE HERT, C.A.O. nr 81 en advies nr 10/2000 over contrôle van Internet en e-mail , *R.W.,* 2002-2003, n°33, p. 1285 ; O. RIJKAERT, Le contrat de travail face aux nouvelles technologies, *Orientations*, 2000, p.210. ;

[129] En effet, il faut constater que d'une part, l'article a été pensé pour les communications téléphoniques et non pour le courrier électronique et que d'autre part, il serait un non sens de ne pas protéger le contenu des communications électroniques entre le POP et le destinataire puisque la majorité des attaques ont lieu à cet endroit et non durant la transmission entre le serveur SMTP et POP.

laquelle je suis partie[130] cela ne tombera pas dans le champ d'application de cet article. Ainsi le fait de diffuser cet enregistrement (de la communication à laquelle je suis partie) à d'autres personnes ne pourra pas être sanctionné sur cette base[131].

Quant au *« contenant »* des communications électroniques, il est protégé par l'article 124 de la loi sur les communications électroniques[132] : *« S'il n'y est pas autorisé par toutes les personnes directement ou indirectement concernées, nul ne peut : 1° prendre intentionnellement connaissance de l'existence d'une information de toute nature transmise par voie de communication électronique et qui ne lui est pas destinée personnellement; 2° identifier intentionnellement les personnes concernées par la transmission de l'information et son contenu; 3° sans préjudice de l'application des articles 122 et 123 prendre connaissance intentionnellement de données en matière de communications électroniques et relatives à une autre personne; 4° modifier, supprimer, révéler, stocker ou faire un usage quelconque de l'information, de l'identification ou des données obtenues intentionnellement ou non. »*

[130] Par exemple une communication téléphonique sur Internet grâce aux systèmes de Voice over Internet Protocol (VOIP) dont le logiciel le plus célèbre est SKYPE.

[131] Par contre, cela pourrait être constitutif d'atteinte à la vie privée de l'autre partie. Cela pourrait également être considéré comme une violation d'une éventuelle clause de confidentialité. Cela pourrait également être constitutif d'infraction au titre de l'article 124 de la loi sur les communications électroniques.

[132] Loi du 13 juin 2005 sur les communications électroniques, *M.B.*, 20 juin 2005. Cette loi est la transposition du cadre réglementaire européen sur les communications électroniques. Pour un commentaire de l'ensemble de la loi voyez Q. COPPIETERS 'T WALLANT, E. LIEVENS, R. QUECK, D. STEVENS, P. VALCKE, Le nouveau cadre réglementaire des communications électroniques : une avancée significative sur un terrain incertain ?, *R.D.T.I.*, 2006, n° 24, p.69 à 105.et plus spécialement p. 93 à 96 sur la protection de la vie privée. Les articles 122 à 133 de la loi sont la transposition de la directive 2002/58/CE sur la vie privée dans le secteur des communications électroniques. Pour un commentaire de cette directive voyez J. DHONT, K. ROSIER, Directive vie privée et communications électroniques : premiers commentaires, R.D.T.I., 2003, n° 15, p. 7- 46.

Cet article, dont la doctrine diverge dans son interprétation, possède potentiellement un champ d'application très large. Bien qu'initialement il n'ait pour objectif que de réglementer les données relatives aux communications électroniques (le « contenant ») et que cette interprétation limitative est renforcée par le fait qu'il est la transposition de la directive 2002/58/CE qui parle des données de trafic et de localisation, par son libellé même, cet article semble pouvoir être interprété de façon à inclure également de façon indirecte le contenu des communications électroniques. Si ces considérations sortent du cadre de la présente contribution, retenons qu'il vise au minimum les données relatives aux communications électroniques, celles de contenant et que les 1° à 3° de l'article n'incriminent que les actes intentionnels alors que le 4° n'exige pas cet élément moral et est par conséquent très large.

L'article 125 prévoit une série d'exceptions à la confidentialité des communications électroniques. Ainsi, lorsque les actes visés à l'article 124 sont accomplis dans le but exclusif de vérifier le bon fonctionnement du réseau et d'assurer la bonne exécution d'un service de communications électroniques, lorsque les actes sont accomplis dans le seul but d'offrir des services à l'utilisateur final consistant à empêcher la réception de communications électroniques non souhaitées, à condition d'avoir reçu l'autorisation de l'utilisateur final à cet effet ou lorsque la loi permet ou impose l'accomplissement des actes visés, l'interdiction prévue à l'article 124 tombera.

Relevons au terme de ce titre II que les CPAS voient leurs communications électroniques, bien protégées, mais qu'à leur tour, la protection du secret des communications électroniques leur impose certains devoirs, en particulier de non contrôle et non interception des communications de leurs employés ou de leurs usagers lorsque ceux-ci utilisent des équipements mis à leur disposition par les CPAS.

Section III
De quelques considérations sur la gestion des moyens informatiques

La partie de l'enquête menée, et en particulier les réponses aux questions posées aux CPAS sur leur intégration à la Banque Carrefour de la Sécurité Sociale, permet de mettre en avant une problématique récurrente dans le domaine du gouvernement électronique : le manque de moyens humains et financiers, le manque d'expertise technique et l'isolement de certaines administrations face à ces nouveaux outils. En effet, l'usage de ces technologies implique nécessairement un coût d'adaptation souvent important. Comment les petites entités administratives peuvent-elles gérer ce coût ? Quelles voies leur sont offertes ? L'externalisation ou la mutualisation de leur informatique peuvent constituer deux solutions dont les avantages respectifs doivent être mesurés. Nous étudierons séparément les questions juridiques soulevées par ces deux solutions.

1. L'externalisation des moyens informatiques

Externaliser[133] peut se définir comme le fait d'avoir recours à une entité tierce afin d'effectuer certaines tâches. Cette notion extrêmement large présente l'avantage de confier à une entité plus qualifiée la réalisation d'une tâche que l'on ne peut accomplir. Cependant, cette pratique peut présenter quelques risques juridiques qu'il ne faut pas sous-estimer.

Concernant la vie privée, la LVP prévoit spécialement cette hypothèse lorsqu'elle envisage la notion de sous-traitant : *« Par "sous-traitant", on entend la personne physique ou morale,*

[133] Ou recourir à l'outsourcing.

l'association de fait ou l'administration publique qui traite des données à caractère personnel pour le compte du responsable du traitement et est autre que la personne qui, placée sous l'autorité directe du responsable du traitement, est habilitée à traiter les données ».

Imaginons par exemple, le cas d'un CPAS qui externaliserait la sauvegarde de ses dossiers informatiques. Une société X serait alors chargée de réaliser à distance une sauvegarde régulière des données à caractère personnel pour le compte du CPAS. Dans ce cas, le traitement dont la finalité est la sauvegarde des données – finalité définie par le CPAS (responsable du traitement) – est réalisé par un sous-traitant, la société X.

Dans cette hypothèse de sous-traitance une série d'obligations supplémentaires trouveront à s'appliquer. Premièrement, le responsable du traitement doit choisir un sous-traitant présentant des garanties techniques et organisationnelles suffisantes[134] pour assurer la sécurité des traitements. D'autre part, le LVP impose au responsable du traitement de prévoir contractuellement un partage clair des responsabilités[135], d'imposer au sous-traitant de n'agir que sur instruction du responsable du traitement et de lui imposer les mêmes obligations que celle que prévoit la LVP. Le responsable du traitement ou son sous-traitant est également tenu d'informer son

[134] Ces mesures doivent assurer un niveau de protection adéquat, compte tenu, d'une part, de l'état de la technique en la matière et des frais qu'entraîne l'application de ces mesures et, d'autre part, de la nature des données à protéger et des risques potentiels.

[135] Article 16 §1 LVP : « § 1er. Lorsque le traitement est confié à un sous-traitant, le responsable du traitement ou, le cas échéant, son représentant en Belgique, doit : 1° choisir un sous-traitant qui apporte des garanties suffisantes au regard des mesures de sécurité technique et d'organisation relatives aux traitements; 2° veiller au respect de ces mesures notamment par la stipulation de mentions contractuelles; 3° fixer dans le contrat la responsabilité du sous-traitant à l'égard du responsable du traitement; 4° convenir avec le sous-traitant que celui-ci n'agit que sur la seule instruction du responsable du traitement et est tenu par les mêmes obligations que celles auxquelles le responsable du traitement est tenu en application du paragraphe 3; 5° consigner par écrit ou sur un support électronique les éléments du contrat visés aux 3° et 4° relatifs à la protection des données et les exigences portant sur les mesures visées au paragraphe 3.

personnel de la législation de protection des données à caractère personnel.

Cependant, si externaliser est une solution au problème des compétences et du temps de travail, cette solution n'est que partielle concernant la problématique du coût. Or le coût constitue l'une des principales préoccupations de l'administration comme le révèle l'enquête menée auprès des CPAS face à leur intégration à la BCSS[136]. Face à cette problématique, il faut donc aller plus loin et envisager la mutualisation.

2. La mutualisation des moyens informatiques

On peut définir la mutualisation comme *« une pratique d'investissements communs à plusieurs utilisateurs rencontrant des besoins similaires, qui bénéficient ainsi de services identiques (ou proches), tout en répartissant la charge de ces investissements »*[137]. Le principal avantage de la mutualisation consiste comme évoqué plus haut dans la réduction des coûts et ce en vertu des économies d'échelle rendues possibles grâce à ce procédé. Mais la mutualisation, permet également, si elle est menée à bien, de favoriser les échanges entre les mutualisants, et par là même, une certaine interopérabilité. Elle permet également aux acteurs de la mutualisation de repenser l'outil informatique, de se l'approprier et de réduire donc leur dépendance vis-à-vis de leur fournisseur informatique. Alors qu'aujourd'hui nous nous trouvons plutôt dans un paradigme où le Fédéral impose des choix technologiques aux entités locales, la mutualisation devrait également permettre de

[136] En effet, 28% des CPAS ayant répondu à cette question citent le coût comme principal inconvénient à leur intégration au sein de la BCSS.

[137] D. DE ROY, *Quelques aspects conceptuels et juridiques de la gestion de l'informatique publique*, à l'occasion du colloque « Services publics et mutualisation informatique : de la théorie à la pratique » organisé par le Parlement de la Communauté française de Belgique, 23 mars 2006, disponible sur http://www.pcf.be/ROOT/PCF_2006/public/evenements/activites_diverses/services_publics_et_mutualisation_informatique/david_de_roy.html

repenser l'informatique du local vers le central. Finalement, elle permet aussi une réduction des risques liés à un éventuel mauvais choix technologique.

Cependant cette pratique présente certains inconvénients. Des inconvénients pratiques résidant dans la conciliation d'intérêts et besoins parfois différents voire opposés. Des inconvénients d'ordre psychologiques tels qu'une réticence psychologique au changement (coût de changement), une défense des privilèges, une volonté de défendre « ses » secrets..

Classiquement la mutualisation peut intervenir à trois niveaux : à propos des développements logiciels, soit en amont (1) soit en aval (2) d'un projet et à propos du matériel informatique (3). En amont, la mutualisation permettra par exemple de partager ses connaissances, de développer en collaboration ou plus simplement de financer ensemble un même projet[138]. En aval, le partage des ressources visera à assurer la maintenance et la mise à jour de son système informatique. En ce qui concerne le matériel informatique, on peut imaginer un CPAS et une commune, par exemple, partageant la même connexion à fibre optique Internet ou encore partageant les mêmes serveurs.

Les autorités administratives ayant recours à la mutualisation – tout comme à l'externalisation – ne doivent cependant pas perdre de vue le principe de continuité. S'il existe des divergences sur la signification de ce principe et sur sa portée, certains auteurs admettent que les usagers peuvent invoquer le principe de continuité vis-à-vis de l'administration. Par conséquent, les usagers auraient la possibilité d'exiger un service continu de l'administration et donc des CPAS. Notre propos n'est pas d'obliger l'administration à garantir un service permanent 7j/7j, 24h/24h mais d'imposer à l'administration une régularité, une permanence dans la disponibilité de ses services.

Ainsi, une administration doit veiller lorsqu'elle s'informatise ou développe de nouveaux outils informatiques à être en mesure de continuer ses services en cas de panne informatique. Pour se faire,

[138] Voy. dans ce sens les projets de mutualisation autour de la communauté plone. Par exemple, www.communesplone.be

l'administration doit posséder les moyens humains et/ou matériels lui permettant de résoudre les éventuelles pannes informatiques. Imaginons une administration totalement informatisée tombant en panne suite à une attaque virale… Comment pourra-t-elle poursuivre sa mission de service public sans que son matériel informatique ne fonctionne ? De même, comment un CPAS pourrait-il continuer à gérer les revenus d'intégration sociale sans connexion à la Banque Carrefour de la Sécurité Sociale ? La prudence est donc de mise…

Par conséquent, une attention toute particulière devra être accordée à une stricte délimitation contractuelle des responsabilités de chacun. Il conviendra également de prévoir des solutions présentant une certaine souplesse et ne créant pas trop de dépendance vis-à-vis de fournisseurs et/ou des partenaires. De plus, l'informatique pouvant être « obscure » à bien des égards aussi bien pour le néophyte que pour l'expert, il convient de se réserver un accès aux codes sources[139] des logiciels utilisés. Sans accès au code source, en cas de faillite du fournisseur informatique (si on a opté pour une externalisation) ou en cas de litige avec les partenaires, l'administration *« mutualisante »* (si on opte pour la mutualisation) pourrait se trouver dans l'impossibilité de *« réparer »* ses logiciels mais aussi de les faire évoluer.

[139] Le code source et le langage de base dans lequel le programme d'ordinateur est écrit.. Il est lisible par l'homme mais non par la machine. Une fois le code source compilé en langage binaire, il s'appelle alors le code objet.

Section IV.
Le formalisme à l'heure du numérique[140]

Depuis la création du code civil, notre système juridique est articulé autour de la notion d'écrit. Suite à la dématérialisation des échanges induite par les technologies de l'information, notre système juridique s'est retrouvé confronté à un problème majeur : quelle force probante, quelle valeur juridique accorder aux *« écrits »*, aux *« documents »* électroniques ? Certaines questions ont dès aujourd'hui trouvé une réponse alors que d'autres restent sans solution.

Cette section se compose de deux parties. La première traite de la force probante des écrits électroniques alors que la deuxième pose la question de la valeur d'un écrit électronique.

1. La force probante d'un écrit électronique

La question que nous soulevons ci dessous présente de multiples facettes : un courriel peut-il être reçu en justice comme mode de preuve ? Quelle est la valeur probante d'un courrier électronique ? Que peut-il prouver? Que ne peut-il pas prouver ? Cette question est d'une importance capitale puisque bien qu'un contrat puisse naître du simple échange des consentements (principe du consensualisme), en cas de litige, il sera considéré comme inexistant si on ne peut le prouver en justice.

Dans un premier temps, il faut opérer une distinction entre trois types de preuves : les preuves pénales, commerciales et civiles. Nous examinerons ensuite un cas bien concret : celui de la signature électronique.

[140] Cette section est à jour au 1er septembre 2006. Elle ne tient pas compte des législations qui auraient pu intervenir depuis.

1.1. La preuve pénale

Concernant la recevabilité, en matière pénale, tout élément de preuve rationnel est en principe admis[141] à condition qu'il ait été valablement recueilli c'est-à-dire sans violation de dispositions légales. A propos de la force probante de ces éléments de preuve, il faut, mais il suffit, que les éléments de preuve emportent l'intime conviction du juge. Dans cette appréciation, le juge est souverain. Un courrier non signé qui n'aurait pas reçu de force probante en matière civile (voy. *infra*) pourrait donc être considéré comme une preuve déterminante en matière pénale.

1.2. La preuve commerciale

Le régime de la preuve libre s'applique entre commerçants. Le code du commerce définit les commerçants comme *« ceux qui exercent des actes qualifiés commerciaux*[142] *par la loi et qui en font leur profession habituelle soit à titre principal, soit à titre d'appoint »*[143]. Cependant pour que ce régime de la preuve libre s'applique, il faut et il suffit que la personne contre qui on veut prouver un acte puisse être qualifiée de commerçant[144]. Il pourra donc arriver que l'administration soit considérée comme commerçant, ce qui sera le cas lorsqu'elle offre des services excédant sa mission de service public, ainsi du logement pour personnes âgées, des repas à domicile ou qu'elle soit amenée à traiter avec des commerçants.

Le régime de la preuve libre signifie que le juge apprécie souverainement la recevabilité et la force probante des éléments de preuve qui lui sont soumis[145]. Cela signifie également que l'on peut

[141] O. LEROUX, Y. POULLET, « En marge de l'affaire Gaia : de la recevabilité de la preuve pénale et du respect de la vie privée », *R.G.D.C.*, 2003, liv. 3, pp. 163 et s. et les références mentionnées.

[142] Pour une définition de l'acte de commerce voyez l'article 2, 2bis et 3 du Code de commerce.

[143] Article 1er du Code de commerce.

[144] Voy. entre autre, Cass. 7 mai 1908, *Pas.*, p. 174 ; 18 janvier 1990, *Pas.*, p. 592.

[145] Sauf régimes légaux dérogatoires

prouver un acte par toute voie de droit, même contre un écrit signé. Par conséquent et sauf cas particuliers, un courriel sera reçu en justice. Sa force probante sera souvent assez forte et dépendra d'une série d'éléments : habitude des parties quant aux modes de conclusion des contrats ; intégrité et inaltérabilité de l'élément de preuve ; lisibilité ; autres modes de preuve pouvant compléter le courriel, etc.

Nous recommandons toutefois à l'administration d'utiliser les mêmes garanties en matière commerciale qu'en matière civile et ce afin d'éviter toute incertitude juridique.

1.3. La preuve civile

1.3.1 Principes généraux

En matière civile, et ce sera le régime applicable dans la plupart des activités des CPAS, la preuve est régie par les articles 1315 à 1369 du Code civil. En l'absence de régime probatoire conventionnel[146] (c'est à dire défini par les parties), il faut se référer au régime probatoire légal. Ces dispositions prévoient un ensemble cohérent appelé « hiérarchie des modes de preuve ». Celui-ci s'articule autour de la notion d'écrit. Au sommet de la hiérarchie se trouve l'acte authentique ou acte notarié. Ensuite, il existe ce que l'on qualifie d'acte sous seing privé, c'est à dire un acte conclu entre particuliers et signé. Si l'acte n'est pas signé, il ne constituera qu'un commencement de preuve par écrit et devra être complété par d 'autres modes de preuve c'est à dire des témoignages, présomptions et aveux.

La disposition centrale de ce régime est l'article 1341 du Code civil qui stipule que *« Il doit être passé acte devant notaires ou sous signature privée, de toutes choses excédant une somme ou valeur de 375 €, même pour dépôts volontaires ; et il n'est reçu aucune preuve par témoins contre ou outre le contenu aux actes, ni sur ce qui serait allégué avoir été dit avant, lors ou depuis les actes, encore*

[146] On vise l'hypothèse où les parties décident de commun accord les formes qui feront office de preuve en cas de contestation future.

qu'il s'agisse d'une somme ou valeur moindre de 375 €. Le tout sans préjudice de ce qui est prescrit dans les lois relatives au commerce. »

Pour le sujet qui nous intéresse, nous mettrons en exergue certaines règles :

- Pour prouver un acte inférieur à 375 €, un écrit n'est pas nécessaire.
- Pour prouver un acte supérieur à 375 €, le Code civil exige soit un acte sous seing privé, soit un acte authentique.
- Si un acte sous seing privé est invoqué, on ne pourra faire preuve contre cet acte que par un autre écrit signé même si la valeur de l'acte est inférieure à 375€

Par conséquent, afin que l'administration puisse s'appuyer sur des éléments de preuve solide, il serait souhaitable de se réserver comme moyen de preuve des écrits signés et ce même pour un acte inférieur à 375€

La doctrine[147] s'accorde majoritairement à considérer que la notion d'écrit est indépendante de son support. Par conséquent et suivant la théorie des équivalents fonctionnels consacré par l'article 16 de la loi du 11 mars 2003[148], un courriel pourra être considéré comme un écrit s'il rencontre les fonctions dévolues à un *« écrit*

[147] Voy . E. MONTERO, M. DEMOULIN, « le formalisme contractuel à l'heure du commerce électronique », *Commerce électronique : de la théorie à la pratique*, Cahier du CRID n°23, Bruxelles, Bruylant, 2003, p. 176 et les références citées : M. FONTAINE, « La preuve des actes juridiques et les technologies nouvelles », in La preuve, colloque U.C.L., 1987, p.18 ; M. ANTOINE, D. GOBERT, « Pistes de réflexion pour une législation relative à la signature digitale et au régime des autorités de certification », *R.G.D.C.,* 1998, n° 4/5, p. 291 ; A. PRÜM, « L'acte sous seing privé électronique : réflexions sur une démarche de reconnaissance », in Mélanges Michel Cabrillac, Paris, Litec, 1999, p. 267. Pour une étude approfondie du concept d'écrit au regard des nouvelles technologies, voy. D.GOBERT, E. MONTERO, « L'ouverture de la preuve littérale aux écrits sous forme électronique », *J.T.*, 2001, spéc. pp. 117-119 ; D.MOUGENOT, « Faut-il insérer une définition de l'écrit dans le code civil ? », *Revue Ubiquité*, 2000, pp. 121-128.

[148] Loi sur certains aspects juridiques de la société de l'information, *M.B.*, 17 mars 2003

classique »[149]. *« L'exigence d'un écrit est satisfaite par une suite de signes intelligibles et accessibles pour être consultés ultérieurement, quel que soit leur support et leurs modalités de transmission. ».* Cependant, si un courrier électronique peut être considéré comme un écrit, encore faut-il qu'il soit signé.

Il est donc indispensable de se pencher sur la valeur d'une signature électronique.

1.3.2 Quelle est la valeur d'une signature électronique ?

1.3.2.1 Qu'est-ce qu'une signature électronique ?

Suite à l'adoption de la directive sur les signatures électroniques[150] et à sa transposition dans notre droit national, la signature électronique est reconnue en droit belge.

La transposition de cette directive européenne en Belgique fut réalisée via différents textes. Une première loi, ayant pour objet de modifier le droit de la preuve en insérant dans l'article 1322 du Code civil la signature électronique en second alinéa, fut édictée le 20 octobre 2000[151].Ce cadre légal fut complété par la loi du 9 juillet 2001[152] qui fixe certaines règles relatives au cadre juridique des signatures électroniques et des services de certification. Un arrêté royal, organisant le contrôle et l'accréditation des prestataires de

[149] Il faut remarquer que si la majorité de la doctrine est unanime sur la distinction entre l'écrit et son support, elle l'est beaucoup moins sur les fonctions dévolues à l'écrit. Voy. les références citées à la note précédente.

[150] Directive 1999/93/CE du Parlement européen et du Conseil du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques, *J.O.C.E.*, L 13/12 à 20 du 19 janvier 2000.

[151] Loi du 20 octobre 2000 introduisant l'utilisation des moyens de communication et de la signature électronique dans la procédure judiciaire et extrajudiciaire, *M.B.*, 22 décembre 2000.

[152] Loi du 9 juillet 2001 fixant certaines règles relatives au cadre juridique pour les signatures électroniques et les services de certification, *M.B.*, 29 septembre 2001, pp. 33070-33078.

service de certification qui délivrent des certificats qualifiés, fut adopté le 6 décembre 2002[153].

Une signature électronique est définie comme une *« donnée sous forme électronique jointe ou liée logiquement à d'autres données électroniques et servant de méthode d'authentification*[154] *».*

Cette définition est technologiquement neutre c'est à dire qu'elle ne vise pas une technologie particulière. Par conséquent, elle vise à la fois les signatures dites numériques à cryptographie symétrique (le destinataire et l'émetteur disposent de la même clé secrète pour les tiers) et asymétrique (l'émetteur dispose d'une clé privée secrète et d'une clé publique, de même que le destinataire). Le chiffrement par l'émetteur d'un condensé du message par sa clé privée et la clé publique du destinataire peut être décrypté par l'utilisation par le destinataire de la clé publique de l'émetteur et de sa propre clé privée, ou encore les signatures biométriques basées sur un élément physique de la personne émettrice (reconnaissance de l'iris, de l'empreinte digitale, etc.). L'objectif de la neutralité technologique est de permettre au droit de suivre les diverses évolutions technologies de façon la plus ouverte possible, par des dispositions susceptibles d'accueillir ces évolutions sans nécessité de révision des dispositions réglementaires.

1.3.2.2 Quelle est la valeur d'une signature électronique ?

Une nouvelle distinction s'impose entre d'une part la recevabilité d'un mode de preuve en justice (un juge peut-il ou non examiner un élément de preuve ?) et d'autre part sa force probante (le juge est-il tenu d'accorder une certaine force probante à un élément de preuve ?).

[153] A.R. du 6 décembre 2002 organisant le contrôle et l'accréditation des prestataires de service de certification qui délivrent des certificats qualifiés, *M.B.*, 17 janvier 2003, pp. 1541-1544.

[154] Art. 2 de la L du 9 juillet 2001 fixant certaines règles relatives au cadre juridique pour les signatures électroniques et les services de certification, *M.B.*, 29 septembre 2001, pp. 33070-33078 et art.2 de la directive 1999/93/CE, *précitée*.

Deux grands principes gouvernent cette matière : le principe de non-discrimination qui interdit à un juge d'écarter une signature parce qu'elle est électronique (recevabilité) et le principe d'assimilation qui oblige à certaines conditions, le juge à accorder la même force probante à une signature électronique qu'à une signature manuscrite.

Concernant le principe dit de non-discrimination, l'article 4, §5 de la loi du 9 juillet 2001[155] stipule qu'*« une signature électronique ne peut être privée de son efficacité juridique et ne peut être refusée comme preuve en justice au seul motif : - que la signature se présente sous forme électronique, […] ».* Toute signature électronique devra donc être reçue en justice sous réserve bien entendu des règles de recevabilité que l'on pourrait qualifier de *« classiques ».*

Mais lorsqu'un écrit électronique est signé au moyen d'une signature électronique, sa valeur probante diffère selon le type de signature utilisée. Certaines catégories de signatures sont en effet totalement assimilées à une signature manuscrite tandis que pour d'autres, il faudra convaincre le juge du fait que la signature remplit certaines fonctions précisées à l'article 1322 du Code civil. C'est à ce stade qu'intervient alors le principe d'assimilation ou d'équivalence. Ce principe ne vaut cependant que pour certain types de signatures (dites « signatures avancées ») comme le précise l'article 4, § 4 de la loi du 9 juillet 2001[156] : *« Sans préjudice des articles 1323 et suivants du Code civil, une signature électronique avancée réalisée sur la base d'un certificat qualifié et conçue au moyen d'un dispositif sécurisé de création de signature électronique, est assimilée à une signature manuscrite, qu'elle soit réalisée par une personne physique ou morale. ».*

Nous insistons : l'assimilation des signatures électroniques aux signatures manuscrites n'existera que pour la *« signature électronique avancée*[157] *réalisée sur la base d'un certificat qualifié*[158]

[155] L du 9 juillet 2001 fixant certaines règles relatives au cadre juridique pour les signatures électroniques et les services de certification, *précitée.*

[156] ibidem.

[157] Est une signature électronique avancée *« une donnée électronique, jointe ou liée logiquement à d'autres données électroniques, servant de méthode d'authentification et satisfaisant aux exigences suivantes :*

et conçue au moyen d'un dispositif sécurisé de création de signature électronique[159] *».*

Une signature électronique ne peut être refusée en justice au motif qu'elle est électronique.

Une signature électronique avancée réalisée sur la base d'un certificat qualifié et conçue au moyen d'un dispositif sécurisé de création de signature électronique est assimilée à une signature manuscrite.

D'un point de vue pratique, nous conseillons à une administration comme un CPAS d'opérer une distinction entre les courriels de faible importance (réponses informelles, échange de courrier interne, simple information aux citoyens ne liant pas l'administration, etc..) et les courriels officiels (conclusion de contrat, réponse liante à une demande, etc..). Il faut toutefois veiller à insérer dans les courriers électroniques de faible importance un *« disclaimer »* précisant que le message n'engage pas l'administration et ne saurait engager la responsabilité de l'administration. A ce propos, on rappelle que l'enquête révèle que seuls 8,73 % des CPAS utilisent ce type de clause.

a) être liée uniquement au signataire ;

b) permettre l'identification du signataire;

c) être créée par des moyens que le signataire puisse garder sous son contrôle exclusif;

d) être liée aux données auxquelles elle se rapporte de telle sorte que toute modification ultérieure des données soit détectée. »

[158] Il s'agit d'un certificat ayant un contenu minimal prévu par la loi (annexe I de la loi du 9 juillet 2001) et émis par un prestataire de service de certification respectant un ensemble de conditions strictes consacrées par la loi (annexe II de la même loi) ;

[159] Un dispositif de création de signature n'est considéré comme sécurisé que s'il satisfait aux exigences de l'annexe III de la loi du 9 juillet 2001.

Si pour les premiers, un courrier électronique signé au moyen d'une signature électronique avancée n'est pas primordial (bien que cela puisse garantir l'identité de la personne émettrice du message par exemple), il est par contre fortement conseillé sinon indispensable d'utiliser cette signature avancée pour les courriels officiels. En effet, premièrement, lorsqu'il faut une signature hors ligne, il en va de même en ligne. Deuxièmement, ces signatures électroniques garantissent à la fois l'identité[160] de l'émetteur du message, le contenu du message et son intégrité.

2. Le formalisme « ad validatem » face à l'écrit et aux formulaires électroniques

Que doit faire un CPAS lorsqu'il reçoit une demande d'aide sociale par courrier électronique ? Doit-il considérer celui-ci comme un « écrit classique » et ainsi répondre dans un délai précis ? La responsabilité d'un CPAS se verra-t-elle engagée s'il ne répond pas ou répond incorrectement à cette demande d'aide sociale ? C'est de cette question d'importance majeure pour les administrations que nous traitons dans cette section.

Prenons une illustration concrète : l'article 58 de la loi organique des CPAS.

« § 1er. Une demande d'aide sociale, soumise à la décision du centre, est inscrite le jour de sa réception, par ordre chronologique, dans le registre tenu à cet effet par le centre public d'aide sociale. La demande écrite est signée par l'intéressé ou par la personne qu'il a désignée par écrit. Lorsque la demande est orale, l'intéressé ou la personne désignée par écrit signe dans la case ad hoc du registre visé à l'alinéa 1er.

§ 2. Le centre adresse ou remet le même jour un accusé de réception au demandeur.

[160] Sur ce point, il faut toutefois remarquer que c'est l'identité « personnelle » de l'émetteur qui est garantie et non sa fonction au sein de l'administration.

§ 3. Lorsqu'un centre public d'aide sociale reçoit une demande d'aide pour laquelle il ne se considère pas compétent, il transmet cette demande dans les cinq jours calendrier par écrit au centre public d'aide sociale qu'il estime être compétent. Dans le même délai, il avertit le demandeur par écrit de cette transmission.

A peine de nullité, la transmission de la demande au centre public d'aide sociale considéré comme étant compétent, ainsi que la notification au demandeur de la transmission, se fait au moyen d'une lettre mentionnant les raisons de l'incompétence. […] ».

Comment satisfaire ces exigences de forme assurément prévues pour le monde papier dans un monde électronique, virtuel ?

Dans un premier temps, remarquons que contrairement à la clause insérée dans le code civil à propos de la force probante de l'écrit en tant que mode de preuve, il n'existe pas de clause générale en matière de « formalisme ad validatem ». Ensuite, et contrairement aux Français, nous ne possédons pas de clauses transversales spécifiques au secteur administratif ou aux relations administrations-citoyens[161].

Certes, en Belgique, il existe la loi du 11 mars 2003 sur certains aspects juridiques des services de la société de l'information[162] qui traite de cette question. En effet, dans ses articles 16 et 17, elle prévoit que *« Toute exigence légale ou réglementaire de forme relative au processus contractuel est réputée satisfaite à l'égard d'un contrat par voie électronique lorsque les qualités fonctionnelles de cette exigence sont préservées. »* Cette disposition envisage bien les questions de forme mais limite son champ aux exigences relatives au processus contractuel. De plus, l'article 17 prévoit des

[161] Voy. Ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives, J.O.R.F., 9 décembre 2005.

[162] Loi du 11 mars 2003 que certains aspects juridiques des services de la société de l'information, M.B., 17 mars 2003. Cette loi est la transposition de la Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur («directive sur le commerce électronique»), *J.O.C.E.*, n° L 178,17 juillet 2000, p. 0001 – 0016.

exclusions supplémentaires : « *L'article 16 n'est pas applicable aux contrats qui relèvent d'une des catégories suivantes : […] 2° les contrats pour lesquels la loi requiert l'intervention des tribunaux, des autorités publiques ou de professions exerçant une autorité publique […].* ». Par conséquent, cette clause appliquant la « théorie des équivalents fonctionnels » aux contrats électroniques conclus sur Internet ne pourrait s'appliquer à propos des administrations. L'approche dite de l'équivalence fonctionnelle repose alors sur une analyse des objectifs et des fonctions de l'exigence légale de forme, que l'administration impose. Cette analyse faite, il s'agit de rechercher, tout en respectant la neutralité technologique, les moyens électroniques qui permettent d'assurer l'accomplissement de ces objectifs[163]. Une étude récente du CRID signale pas moins de onze catégories d'exigences formelles[164] présentes dans les formulaires ou documents de l'administration.

Nous nous trouvions donc jusqu'il y a peu face à un vide juridique concernant la valeur légale d'un courrier électronique reçu par l'administration. Il est urgent que ce vide juridique soit comblé. En effet, comment peut-on envisager une gouvernance électronique sans régler cette question ? Comment créer une gouvernance électronique si les citoyens ne sont pas assurés de la *« valeur »* des messages électroniques envoyés à l'administration ? De plus, l'administration est tenue par les « lois du changement » l'obligeant

[163] Sur cette théorie, son intérêt et sa consécration en droit belge par l'article 16 de la loi du 11 mars 2003, lire entre autres : M. Demoulin et E. Montero, «La conclusion des contrats par voie électronique», *in* M. Fontaine (sous la directionde), *Le processus de formation du contrat. Contributions comparatives et interdisciplinaires à l'harmonisation du droit européen*, Bruxelles, Bruylant et Paris, L. G. D. J.,2002, p. 716, n° 32. Pour plus de développements sur la théorie des équivalents fonctionnels, voy. D. Gobert et E. Montero, *La signature dans les contrats et les paiements électroniques: l'approche fonctionnelle*, D. A./ O. R., 2000, n° 53, pp. 17- 39

[164] Ainsi, sont envisagées : 1. la signature ; 2.l'apposition d'un sceau officiel ou d'un cachet ; 3.le paraphe de chaque page du formulaire et des documents annexés ;4.la mention manuscrite «lu et approuvé» ;5.la date précédant la signature ; 6. l'exigence de biffer la mention inutile ; 7. les formulaires requérant l'intervention de plusieurs personnes/entités différentes ; 8. les documents en tout genre à annexer au formulaire ; 9. l'envoi du formulaire ou d'un document en plusieurs exemplaires ; 10. la confidentialité de certaines données fournies ; 11. les exigences relatives à l'envoi du formulaire.

à s'adapter à son environnement. Le numérique étant de plus en plus présent dans les foyers, il serait opportun que l'administration s'adapte et intègre ces nouveaux modes de communications électroniques.[165]

Heureusement, une prise de conscience politique semble avoir eu lieu. En effet, le Conseil des Ministres au niveau fédéral a récemment créé une « Charte à destination de l'administration » intitulée : *« Charte pour une administration à l'écoute des usagers »*[166]*.* Cette Charte a, entre autres, pour objectif d'adapter l'administration aux technologies de l'information. Si l'usage d'une circulaire est à priori critiquable (voyez supra nos réflexions à propos de la circulaire émise par la BCSS) car d'une force légale très faible[167], on ne peut que se féliciter du contenu de cette initiative. Comme le communiqué de presse du Conseil des Ministres le

[165] Attention cependant à ne pas tomber dans l'extrême inverse et à obliger les usagers de l'administration à communiquer ou poser des actes vis-à-vis de l'administration uniquement par voir électronique. Cela serait en effet contraire au principe d'égalité et de non-discrimination. A noter en ce sens, l'article 4 § 1 de la loi du 9 juillet 2001 fixant certaines règles relatives au cadre juridique pour les signatures électroniques et les services de rectification, *M.B.*, 29 septembre 2001 : « *A défaut de dispositions légales contraires, nul ne peut être contraint de poser un acte juridique par voie électronique.* »

[166] Bientôt coulée dans les formes d'une circulaire et publiée au Moniteur Belge. Voyez http://www.belgium.be/eportal/application?pageid=contentPage&docId=42763 , Conseil des Ministres du 23 juin 2006, Améliorer le service au client : l'administration s'engage. Insistons sur le fait que cette charte est créée par l'exécutif à destination des administrations. Cette charte pour une administration à l'écoute des usagers a un objectif et un rôle distinct d'une « charte informatique dont nous traitons au titre VI. Ces deux concepts n'ont pas la même signification. La dernière est un document interne à une administration par lequel l'administration elle-même définit sa politique informatique.

[167] Il restera à se poser la question de la qualification de cette future circulaire. Peut-elle être considéré comme un acte réglementaire ou doit-elle être considérée comme une simple directive donnée à l'administration ? Si elle est considérée comme acte réglementaire, a-t-elle respecté les exigences de validité de ces actes ? Cet acte réglementaire respecte-t-il la hiérarchie des normes ? Dans la négative, sa portée s'en verrait considérablement réduite en cas de recours (article 159 Constitution).

précise: « pour la première fois, une Charte propose des principes communs à tous les services afin de rendre l'administration à la fois plus serviable et plus accessible pour les citoyens et les entreprises »[168]. Ceci semble prendre en compte nos préoccupations énumérées en introduction. Reste à ce que les principes mêmes de cette Charte puissent trouver à s'appliquer dans nos CPAS à travers l'intervention de leur pouvoir de tutelle.

Le contenu de la Charte lui-même mérite sans aucun doute notre attention. Celle-ci est composée de 13 engagements. Nous nous attarderons plus spécifiquement sur certains engagements dans le cadre de cette contribution.

Le point 6 stipule que *« Tout service public autorisera que la communication avec les citoyens ou les entreprises se fasse par le biais de différents canaux tels que le courrier électronique, le courrier, le téléphone et le fax. […]».* Remarquons que le texte ne vise que la communication et non les demandes formelles. Ainsi, suivant cette interprétation, l'administration serait tenue de répondre à une demande de renseignement par voie électronique mais non d'autoriser l'introduction de demandes d'aide sociale par voie électronique.

Deuxième engagement intéressant pour notre propos, le point 7 : *« Pour autant que la communication électronique soit autorisée par les dispositions légales, ni les citoyens ni les entreprises ne pourront être contraints à introduire une demande sur papier si la voie électronique est disponible. ».* Quel sens faut-il donner à cet engagement ? Faut-il comprendre que les demandes ne peuvent-être introduites que si une disposition expresse prévoit (autorise) les demandes électroniques ou qu'à défaut de mentions contraires, les demandes peuvent être envoyées par voie électronique ? Notre enthousiasme nous pousse vers la deuxième possibilité alors que la raison nous amène à considérer la première hypothèse comme la plus plausible. Mais quel est alors l'intérêt de cet engagement si ce n'est d'affirmer que chaque citoyen est autorisé à faire ce que la loi lui permet de faire… ? Valait-il la peine d'insérer cet engagement qui serait alors dépourvu de sens ?

[168] *Ibidem*

Dernier point de cette Charte méritant d'être mentionné pour nos propos: *« 9. Tout service public répondra aux courriers électroniques et aux lettres en empruntant les mêmes voies, à moins que les données soient de nature à déconseiller toute communication électronique […].»… « Si un service public est contacté pour information ou pour une demande par voie électronique (conformément aux points 6 et 7), il sera dans l'obligation de répondre via le même mode de communication sauf si les données sont de nature à déconseiller toute communication électronique ».* La formulation du principe est claire mais que vise la finale de cette disposition ? Il est évident que l'on voit mal comment une administration pourrait par exemple délivrer un permis de conduire ou une carte d'identité par voie électronique. Cependant doit-on interpréter cette finale comment excluant des documents contenant des données sensibles au motif qu'ils pourraient par exemple être facilement interceptés par voie électronique ? Nous ne le pensons pas. En effet, il est techniquement possible de garantir un niveau de sécurité suffisant via l'utilisation de signature électronique à cryptographie asymétrique. Cela requiert cependant que les deux correspondants possèdent chacun une signature avancée. La signature de l'expéditeur permettra de garantir que le document émane bien de l'administration alors que celle du destinataire permettra de garantir la confidentialité du document. Si l'administration ne pourra se « cacher » derrière le fait qu'elle ne possède pas de signature pour éviter ce mode de communication, on peut par contre considérer comme légitime que l'administration refuse l'envoi par voie électronique si le destinataire ne possède pas de signature électronique permettant de crypter le message et ainsi de garantir sa confidentialité.

Si cette Charte présente une avancée certaine, pour les différentes raisons énumérées ci-dessus, elle ne pourrait se substituer à une clause transversale en matière administrative. La nécessité de trouver des équivalents fonctionnels aux référents papiers est chaque jour de plus en plus pressante. Au niveau de la Région wallonne, heureusement un décret a été pris le 14 décembre 2006[169]. Son titre est explicite : *« Décret relatif à la reconnaissance*

[169] M.B. 27 décembre 2006, p. 74735. Et l'exposé des motifs (Parlement Wallon, Session 2006-2007, 6 oct. 2006, Doc. 467 (2006-2007), n°1

juridique des formulaires électroniques de la Région wallonne ». Un article unique stipule :

« Article 1er. Un formulaire électronique de la Région wallonne complété, validé et transmis, avec ses éventuelles annexes, conformément aux modalités et conditions définies par le Gouvernement, est assimilé au formulaire papier portant le même intitulé, complété, signé et transmis, avec ses éventuelles annexes, à l'administration concernée, conformément aux dispositions décrétales et réglementaires. »

Si la solution transversale proposée par la Région wallonne, solution qui attend encore ses arrêtés d'application, apparaît s'imposer non seulement aux formulaires émis par les autorités régionales mais également par les autorités qui traitent des matières relevant de la compétence de la Région et dans le cadre des opérations relevant de telles compétences, on note, avec le Conseil d'Etat[170], que les matières traitées par le CPAS qui ne relèvent pas d'une telle compétence sont exclues du champ d'application du décret wallon. En d'autres termes, suivant que la matière traitée relève ou non de la compétence régionale, le CPAS sera autorisé à bénéficier de la solution souple wallonne mais celle-ci est exclue pour des compétences relevant d'autres pouvoirs comme les Communautés et l'Etat fédéral. Une fois de plus, le CPAS risque donc d'être victime de la multiplicité des échelons de pouvoir qui régissent son activité.

Sans doute, peut-on imaginer que les CPAS ayant répertorié l'ensemble des contraintes rencontrées puissent proposer aux gouvernements[171] en fonction de leur compétence, les solutions

[170] Avis L 40.983/2/V publié en annexe du projet de loi : Le Gouvernement wallon ne pourra donc trouver, dans ces dispositions, une habilitation pour prendre les mesures qu'elles prévoient, dans des matières communautaires. En effet, la Constitution et les autres dispositions de réformes institutionnelles établissent une nette distinction entre les matières régionales et les matières communautaires et, comme le Conseil d'Etat l'a souvent rappelé, un même décret de la Région wallonne ne peut régler des matières régionales et des matières communautaires

[171] L'article 16 § 3 réserve cette compétence au Roi en matière civile du moins. En matière administrative, c'est, nous semble-t-il, l'instance compétente vis-à-vis de l'opération à la base de la transaction administrative qui devrait se prononcer (ex. les exigences de formalisme administratif reprises dans les

dégagées dans le cadre de la réglementation wallonne. Dans le cadre des CPAS, ceci mérite sans nul doute une réflexion au niveau local qui devrait pouvoir s'appuyer sur une institution régionale les représentant et faisant remonter l'information aux parlementaires. Chaque solution a en effet ses avantages et ses lourdeurs… même dans l'environnement numérique…

règlements sur la tutelle administrative des CPAS doivent être réglées par le niveau régional).

Section V
Une charte informatique[172] pour les CPAS dans leurs relations avec leurs agents: pourquoi, comment ?

1. Pourquoi créer une charte informatique dans un CPAS ?

Une charte informatique a pour objectif d'informer les utilisateurs sur les conditions d'utilisations et les usages abusifs des outils informatiques mis à leur disposition dans le cadre de leur fonction. Dans cette optique, elle détermine les conditions d'accès au réseau et fixe les procédures d'utilisation du courrier électronique et de l'Internet en précisant les sanctions éventuelles encourues par le personnel y dérogeant. Elle permettra dès lors d'identifier plus précisément les responsabilités respectives des agents et de l'administration.

[172] La Charte dont nous évoquons ici la possible existence serait spécifique aux CPAS et pourrait sur certains points reprendre des éléments de la « Charte » adoptée par le présent gouvernement et commentée sur certains points supra dans le titre V.

Sur les chartes informatique voy. L. DEPLANQUE, C. LOBET_MARIS, F. NAVARRE, POULLET Y., *Vous avez un message…, Administration publique et courrier électronique, Guide des bonnes pratiques*, Presses universitaires de Namur, 2004, 150 pp. et plus spécialement pp.61-69.

Voy également le travail de l'Union des Villes et Communes réalisé parallèlement une étude menée par le C.R.I.D. (Aspects organisationnels et juridiques du courrier électronique dans les relations administrations-citoyens, disponible sur http://www.fundp.ac.be/recherche/projets/page_view/04925305/) et le modèle de Charte informatique proposé ainsi que les notes explicatives, http://www.uvcw.be/publications/modeles/modele-882.htm

On note que dès à présent 19% des CPAS ont créé une charte informatique[173]. Par ailleurs, l'Union des Villes et Communes a, en dialogue avec les communes, mis au point une charte modèle applicable aux relations entre agents des communes et usagers des services communaux, d'une part et communes, d'autre part.

2. Quel sera le statut de la charte informatique ?

Une charte informatique crée t-elle des obligations? Suivant la qualité des personnes visées par la charte, l'administration, le CPAS dans le cas qui nous concerne, a plusieurs possibilités pour créer et rendre obligatoire la charte informatique.

- Soit il est choisi de donner à la charte un statut de règlement de travail. Pratiquement plusieurs méthodes permettent de conférer le statut de règlement de travail à la charte informatique : inclusion totale, annexion ou renvoi exprès au règlement de travail. Afin d'éviter d'encombrer le règlement de travail nous recommandons l'annexion ou le renvoi exprès. Cette possibilité vaudra pour le personnel contractuel mais aussi pour le personnel sous statut car depuis le 01 juillet 2003, les travailleurs sous statut peuvent également voir leur emploi régi par un règlement de travail[174].
- Soit il est opté pour une intégration de la charte au contrat de travail ou un renvoi à cette charte dans ce contrat de travail. La charte aura alors un statut contractuel.
- Soit il est décidé de ne pas entreprendre d'autres démarches que la diffusion de la charte. Celle-ci sera alors considérée comme une directive imposée aux membres de l'administration ou une encore comme une règle déontologique.

[173] Cf. notre enquête, publiée dans le rapport se trouvant sur le site http://www.fundp.ac.be/pdf/publications/57376.pdf

[174] Loi du 18 décembre 2002 modifiant la loi du 08 avril 1965 instituant les règlements de travail, *M.B.*, 14 janvier 2003, p. 01106.

3. Quel sera le processus d'adoption à respecter pour rendre la charte obligatoire ?

La procédure d'adoption de cette charte informatique sera différente, selon le caractère statutaire ou contractuel des agents. Concernant les agents sous statut, deux possibilités s'offrent pour leur imposer le contenu de la charte informatique :

3.1. Considérer la charte comme une règle déontologique ou comme une directive

Le statut des agents de l'Etat est régi par l'Arrêté Royal du 2 octobre 1937[175]. Ce texte prévoit dans son article 7 que : *« Les agents de l'Etat remplissent leurs fonctions avec loyauté, conscience et intégrité sous l'autorité de leur supérieur hiérarchique. A cet effet, ils doivent : 1° respecter les lois et règlements en vigueur ainsi que les directives parmi lesquelles les règles de déontologie, de l'autorité dont-ils relèvent ; […] ».* L'article 13 de ce même Arrêté Royal prévoit que *« toute contravention aux articles 7 […] est punie suivant l'exigence des cas, de l'une des peines disciplinaires prévues par l'article 77, sans préjudice des lois pénales ».* On peut déduire de ces dispositions que la charte informatique sera obligatoire pour les agents sous statut, que cette charte soit émise sous la forme d'une simple directive ou soit simplement considérée comme une règle de déontologie.

Si on opte pour le statut de règle déontologique ou de directive, plusieurs possibilités s'offrent à l'employeur pour porter à la connaissance du travailleur ces nouvelles directives ou règles déontologiques. Il devra cependant veiller à pouvoir apporter la preuve de cette diffusion en cas de litige.

On peut à titre illustratif citer différents procédés. Par exemple, la charte peut être diffusée sur l'Intranet de l'administration (il est alors important de veiller à ce que l'ensemble des travailleurs des CPAS soient avertis de l'existence de cette charte et que chacun ait accès

[175] Arrêté Royal du 2 octobre 1937 portant le statut des agents de l'Etat, *M.B.*, 8 octobre 1937, p. 6073.

à l'Intranet) ou envoyée au domicile de chaque fonctionnaire en version papier ou encore être distribuée sous forme papier à chaque fonctionnaire lors de l'octroi des codes d'accès aux réseaux de communication. On peut aussi imaginer qu'à chaque ouverture de session effectuée par un fonctionnaire à partir de son PC, un message rappelant la nécessité de respecter la charte apparaisse. Ce message serait alors accompagné d'un lien permettant de prendre effectivement connaissance de la charte informatique.

3.2. Inclure la charte, l'annexer ou y faire un renvoi dans le règlement de travail

Une autre possibilité pour rendre obligatoire la charte vis-à-vis des agents sous statut est d'incorporer, d'annexer ou de faire un renvoi à la charte dans le règlement de travail car depuis le 1er juillet 2003, les travailleurs sous statut peuvent également voir leur emploi réglé par un règlement de travail[176].

S'il est opté pour une intégration de la charte informatique au règlement de travail, une phase de concertation devra avoir lieu. En effet, une modification du règlement de travail à propos de l'usage du courrier électronique et d'Internet relève de l'organisation du travail et doit donc en principe être soumise à la « négociation ». Cependant puisqu'elle ne fait pas partie des matières visées par l'article 2 de la loi organisant les relations entre les autorités publiques et les syndicats des agents relevant de ces autorités[177], une « concertation » préalable avec les organisations syndicales représentatives suffira et il sera alors possible de « passer outre » l'éventuel refus des organisations syndicales.

Ce règlement devra en vertu de l'article 15 de la loi instituant les règlements de travail recevoir un régime particulier de publicité : un avis affiché dans un endroit apparent et accessible indiquant l'endroit où le règlement de travail et les textes auxquels il fait, le cas

[176] Loi du 18 décembre 2002 modifiant la loi du 8 avril 1965 instituant les règlements de travail, *M.B.*, 14 janvier 2003, p.01106.

[177] Loi du 09 décembre 1974 organisant les relations entre les autorités publiques et les syndicats des agents relevant de ces autorités, *op. cit.*

échéant, référence peuvent être consultés ; chaque travailleur doit pouvoir prendre connaissance en permanence et sans intermédiaire du règlement définitif et de ses modifications dans un endroit facilement accessible et l'employeur doit remettre copie de ce règlement à chaque travailleur.

3.3. Concernant les agents contractuels

Il découle d'une lecture combinée de la loi instituant les règlements de travail[178], de la loi sur le travail[179] et de la loi organisant les relations entre les autorités publiques et les syndicats des agents relevant de ces autorités[180] qu'il existe deux possibilités concernant les agents sous contrats.

Soit inclure la charte informatique dans le règlement de travail ou du moins y faire un renvoi exprès, soit l'insérer dans les contrats individuels. En effet, contrairement aux agents sous statut pour lesquels le statut prévoit des règles particulières à propos des directives ou règles déontologiques, les obligations de la charte ne pourront être sanctionnées que si elles font partie du règlement de travail ou du contrat.

3.4. Inclure la charte, l'annexer ou y faire un renvoi dans le règlement de travail

L'insertion de la charte dans le règlement de travail présente plusieurs avantages :

[178] Loi du 8 avril 1965 instituant les règlements de travail, *M.B.*, 05 mai 1965, p. 01106.

[179] Loi du 16 mars 1971 sur le travail, *M.B.*, 30 mars 1971, p. 03931.

[180] Loi du 9 décembre 1974 organisant les relations entre les autorités publiques et les syndicats des agents relevant de ces autorités, *M.B.*, 24 décembre 1974, p. 15410.

- Une facilité de mise en place : seule une modification du règlement de travail devra être faite. Cela évitera de devoir convoquer un par un l'ensemble du personnel.
- Elle permettra de sanctionner certains comportements du travailleur, jugés abusifs, sans nécessairement être constitutifs d'infractions pénales ou être dommageables pour l'entreprise. Il faudra toutefois veiller à prévoir spécifiquement ces sanctions dans le règlement de travail[181].

3.5. Inclure la charte, l'annexer ou y faire un renvoi au contrat de travail

La deuxième solution est d'inclure la charte informatique dans le contrat de travail, d'y faire référence ou de l'annexer. Dans cette hypothèse, le régime de responsabilité contractuelle classique[182] s'appliquera et, par exemple, la violation de la charte informatique pourra éventuellement être considérée comme un motif grave permettant le licenciement si elle rend immédiatement et définitivement impossible toute collaboration professionnelle entre l'employeur et le travailleur[183].

Dans cette hypothèse, il faudra que chaque agent signe un avenant au contrat. Cette signature sera la manifestation du consentement du travailleur. Une copie de cet avenant devra être délivrée à chaque agent. Il n'y aura pas d'autres mesures de diffusion à prendre.

[181] En effet, l'article 16 de la loi instituant le règlement de travail stipule que « seules les pénalités prévues par le règlement de travail peuvent être appliquées ». Le règlement de travail devra donc prévoir les sanctions appropriées en cas de non respect de cette charte

[182] Article 18 de loi du 03 juillet 1978 relative aux contrats de travail, *M.B.*, 22 août 1978, p.9277.

[183] Article 35 de la loi du 03 juillet 1978 relative aux contrats de travail, *ibidem.*

4. A propos des sanctions

Tout dépendra du statut de la charte informatique :

Si la charte possède un statut contractuel par son inclusion ou un renvoi dans le contrat de travail, les sanctions seront les sanctions classiques en matière de contrat de travail pouvant aller jusqu'au licenciement pour motif grave à condition que la faute rende immédiatement et définitivement impossible toute collaboration professionnelle entre l'employeur et le travailleur[184]. La charte devrait idéalement avoir été signée par le travailleur et il incombera à l'employeur de prouver la faute du travailleur ainsi que de respecter les éventuelles modalités de préavis.

Si elle est annexée ou incorporée au règlement de travail, les sanctions seront celles prévues dans ce même règlement de travail[185].

Si la charte possède le statut de règle déontologique, les sanctions devront être comprises dans celles prévues à l'article 77 de l'Arrêté Royal du 2 octobre 1937 portant le statut des agents de l'Etat[186] : *« § 1er. Les peines disciplinaires suivantes peuvent être prononcées :1° le rappel à l'ordre; 2° le blâme; 3° la retenue de traitement; 4° le déplacement disciplinaire; 5° la suspension disciplinaire; 6° la régression barémique; 7° la rétrogradation; 8° la démission d'office; 9° la révocation. »* La seule condition est que l'agent ait eu connaissance de ces directives ou règles déontologiques. L'employeur devra veiller à préserver la preuve de cette information.

[184] Article 35 de la du 3 juillet 1978 relative aux contrats de travail, *M.B.*, 22 août 1978, p. 9277.

[185] Article 16 de la Loi du 8 avril 1965 instituant les règlements de travail, *M.B.*, 05 mai 1965, p. 5064.

[186] Arrêté Royal du 2 octobre 1937 portant le statut des agents de l'Etat, *M.B.*, 8 octobre 1937 ; Err. *M.B.,* 18-19 octobre 1937, p. 6362.

Conclusion

La présente contribution entend illustrer les diverses questions juridiques que toute administration rencontre à l'occasion de l'utilisation croissante des technologies de l'information et de la communication dans ses relations avec ses usagers. Les CPAS n'échappent pas à la règle. Sans doute, ces questions trouvent-elles dans notre pays des réponses plus ou moins développées : le gouvernement belge s'est montré en effet très volontariste à la fois pour développer l'e-gouvernement mais également pour entourer ce développement de nombreux textes dont l'audace séduit souvent nos voisins. Ainsi, le développement du réseau de la Sécurité Sociale et la multiplication des procédures désormais électroniques entre les membres du réseau, la généralisation à la fois de la carte d'identité et de la signature électroniques qui autoriseront entre les usagers et les CPAS nombre de transactions électroniques, constituent des outils importants de l'efficience administrative et d'un meilleur service aux citoyens.

L'intégration des CPAS dans ce vaste mouvement du gouvernement électronique est récente et sans doute a-t-elle été, même si les exceptions existent, mal préparée. Chaque jour, des applications nouvelles sont mises au point sans que celles-ci n'aient fait l'objet de réflexions préalables et notamment sans que n'aient été identifiées les exigences juridiques liées à ces applications nouvelles. La protection des données à caractère personnel relatives aux usagers et les exigences de sécurité liées à cette protection sont peu maîtrisées par un personnel auquel il est d'abord demandé de l'efficience. Les exigences liées au formalisme administratif, qui ont tout leur sens lorsqu'il s'agit de protéger des usagers faibles, sont difficilement satisfaites par une administration tentée par la facilité que représente le « tout électronique ». Le malaise ressenti lors de cette intégration, malaise vécu d'abord par les gens du terrain, les agents des CPAS en contact direct avec les usagers traditionnels, s'amplifie du fait que les structures communes de réflexion existent peu, chaque CPAS se trouvant isolé. Sans doute, la constitution de plates-formes d'échanges d'expériences voire de solutions logicielles ou d'applications informatiques serait-elle à conseiller.

Notre propos tend à répondre à ce malaise en brossant le contour des solutions légales et en proposant certaines pistes de solution. La mutualisation des expériences voire des ressources apparaît importante pour lutter contre l'isolement des CPAS et faire face à leur taille souvent réduite. La construction en commun (c'est-à-dire avec l'ensemble des CPAS mais également par un dialogue entre les dirigeants de ces CPAS et les agents) d'une charte qui permettrait par un langage convivial de guider chaque agent des CPAS dans la conduite des opérations et dans l'utilisation des ressources nouvelles constitue un autre pilier important d'une maîtrise des technologies de l'information et de la communication.

Bibliographie

Législations et règlements

Convention n° 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, 28 janvier 1981, Strasbourg, disponible sur *http://www.conventions.coe.int/Treaty/Html/108.htm*

Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, J.O.C.E., 23 novembre 1995, L 281 , p. 31 à 50, disponible sur *http://europa.eu/eurlex/fr/index.htm*

Loi du 8 août 1983 organisant un registre national des personnes physiques, M.B., 21 avril 1984.

Loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque Carrefour de la sécurité sociale, M.B., 22 février 1990, p. 03288.

Loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard du traitement de données à caractère personnel, M.B., 27 mars 1991.

Loi du 12 novembre 1997 relative à la publicité des administrations dans les provinces et communes, M.B., 19 décembre 1997.

Loi du 25 novembre 2000 relative à la criminalité informatique, M.B., 03 février 2001.

Loi du 9 juillet 2001 fixant certaines règles relatives au cadre juridique pour les signatures électroniques et les services de certification, M.B., 29 sept. 2001

Loi du 10 février 2003 relative à la responsabilité des et pour les membres du personnel au service des personnes physiques, M.B., 27 mars 2003.

Loi du 13 juin 2005 sur les communications électroniques, M.B., 20 juin 2005.

Décret relatif à la reconnaissance juridique des formulaires électroniques de la Région wallonne, M.B. 27 décembre 2006, p. 74735 et l'exposé des motifs (Parlement wallon, Session 2006-2007, 6 octobre 2006.

A.R. du 13 février 2001 portant exécution de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, M.B. 13 mars 2001.

A.R. du 6 décembre 2002 organisant le contrôle et l'accréditation des prestataires de service de certification qui délivrent des certificats qualifiés, M.B., 17 janvier 2003.

A.R. du 30 novembre 2003 modifiant l'arrêté royal du 25 mars 2003 portant des mesures transitoires relatives à la carte d'identité électronique, M.B., 12 décembre 2003.

A.R. du 4 mars 2005 relatif à l'extension du réseau de la sécurité sociale aux centres publiques d'aide sociale, en ce qui concerne leurs missions relatives au droit à l'aide sociale, en application de l'article 18 de la loi du 15 janvier 1990 relative à l'institution et l'organisation d'une Banque Carrefour de la Sécurité sociale, M.B., 31 mars 2005, p. 13898
Circulaire TC/EC/23.09 du 18 février 2004 concernant la connexion des CPAS à la Banque Carrefour de la Sécurité sociale et la loi du 15 janvier 1990 relative à la protection et à l'organisation de la Banque Carrefour, disponible sur *http://www.mi-is.be/documents/circt&c 18-02.pdf*

UVC, Directives relatives à l'utilisation des moyens de communications électroniques en réseau au sein de la commune/du CPAS/publié sur le site de l'Union de Villes et Communes.

Ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives, JORF, 9 décembre 2005.

Avis n° 99/09 du comité sectoriel de la sécurité sociale du 09 novembre 1999 modifié le 25 juillet 2000 relatif à diverses questions posées par le Ministre des Affaires sociales, de la santé publique et de l'environnement concernant les conseillers en sécurité des centres publics d'aide sociale, disponible sur *http://www.mi-is.be*

http://perso.wanadoo.fr/yves.lafargue/negointranet/telecharge/droits annexe21.doc

http://www.cgtrenault.com/grilles/accords/charteintranet.htm

Commission de la protection de la vie privée : *http://www.privacy.fgov.be*

RIJCKAERT O., juillet 2002, Directive relative à l'utilisation des services internet au sein de l'entreprise.

Doctrine

ANTOINE M., GOBERT D., « Pistes de réflexion pour une législation relative à la signature digitale et au régime des autorités de certification », dans Revue Générale de Droit Civil Belge = Tijdschrift voor Belgisch Burgerlijk Recht, 1998, n° 4-5, pp. 285-310.

BLONDIAU P., La nouvelle loi sur la protection de la vie privée est entrée en vigueur
http : www.uvcw.be/matieres/communication/pb_vie_privee.htm

BOLLEN S., La responsabilité civile des communes et de leurs agents, Union des Villes et Communes, janvier 1998 disponible sur http : www.ucvw.be/matieres/institutions/bollen-responsabilité_civile.htm

BOULANGER M-H, LACOSTE A-C, LOUVEAUX S., La surveillance des communications électroniques des employés, Ubiquité, 2003, n°15, pp.47-69

DEMOULIN M., MONTERO E., « Le formalisme contractuel à l'heure du commerce électronique », dans Commerce électronique : de la théorie à la pratique, Cahiers du Centre de Recherches Informatique et Droit n° 23, Bruxelles, Bruylant, 2003, pp. 131-194.

DEMOULIN M., MONTERO E., « La conclusion des contrats par voie électronique », dans Le processus de formation du contrat : contributions comparatives et interdisciplinaires à l'harmonisation du droit européen, Bruxelles, Bruylant, 2002, pp. 693-788

De ROY D., de TERWANGNE C., POULLET Y., La convention européenne des droits de l'homme en filigrane de l'administration électronique, Actes du colloque organisé par l'ULB, Mars 2006, p. 32.

DE ROY D., « Quelques aspects conceptuels et juridiques de la gestion de l'informatique publique », dans Services publics et mutualisation informatique : de la théorie à la pratique. Compte rendu de la journée organisée le 23 mars 2006, Bruxelles, Parlement de la Communauté française, 2006, pp. 7-14.

de TERWANGNE C., LOUVEAUX S., Protection de la vie privée face au traitement de données à caractère personnel : le nouvel arrêté royal, Journal des Tribunaux, 2001, p. 457 -470.

de VILLENFAGNE F., DUSOLLIER S., La Belgique sort enfin ses armes contre la cybercriminalité : à propos de la loi du 28 novembre 2000 sur la criminalité informatique. http:// www.droit.technologie.org/dossiers/analyse_loi_281101_criminalite_ informatique.pdf

DEOM D., La responsabilité civile des fonctionnaires : une page se tourne, Rev. Dr. comm., 2003, liv.3, pp. 8-29.

DHONT J., ROSIER K., *Directive vie privée et commentaires électroniques : premiers commentaires*, RDTI, 2003, n° 15, p. 7-46.

DELPLANQUE L., LOBET-MARIS C., NAVARRE F., POULLET Y., *Vous avez un message …, Administration Publique et courrier électronique, Guide de bonnes pratiques*, PUN, 2004,147 pages.

GOBERT, D., « Cadre juridique pour les signatures électroniques et les services de certification : analyse de la loi du 9 juillet 2001 », in *La preuve*, Formation permanente CUP, Volume 54, mars 2002, pp. 83-172.

GOBERT, Didier, MONTERO, Etienne, « L'ouverture de la preuve littérale aux écrits sous forme électronique », *Journal des Tribunaux*, 2001, n° 6000, pp. 114-129.

GUINOTTE L ., « La signature électronique après les lois du 20 octobre 2000 et du 9 juillet 2001 », *Journal des Tribunaux*, 2002, pp. 553-562.

HERVEG J., POULLET Y., VERHAEGEN M-N., « Les droits du patient face au traitement informatisé de ses données dans une finalité thérapeutique : les conditions d'une alliance entre informatique, vie privée et santé », *Revue de Droit de l'Université de Sherbrooke*, 2002, n° 2, pp. 56-65.

LEONARD, Th., POULLET, Y., « La protection des données à caractère personnel en pleine (r)évolution », loi du 11 décembre 1998 transposant la directive 95/46/CE du 24 octobre 1995 », *Journal des Tribunaux*, 1999, n° 5928, p. 369.

Les droits et devoirs des gestionnaires de réseau, disponible sur http *: http://www.pisa.belnet.be/pisa/fr/jur/gestionnairesdereseaux.htm*

LIEUTENANT, T., MARIN. S., « Archivage et horodatage de documents électroniques », Mai 2001 disponible sur le site http : *http://www.droit.fundp.ac.be/e-justice/documents/archivage-horodatage.pdf*

Politique de gestion du courrier électronique : des mesures à prendre, 1997, disponible sur le site *http: //www.ebsi.umontreal.ca/cursus/vol3nO1/periat.htm*

MOUGENOT D., « Faut-il insérer une définition de l'écrit dans le code civil ? », *Ubiquité*, 2000, pp.121-128.

POULLET Y., « Mieux sensibiliser les personnes concernés : les rendre acteurs de leur propre protection », Rapport établi pour la conférence du Conseil de l'Europe, organisé les 14 et 15 octobre 2004, Lamy, Droit de l'Informatique, 2005, n° 5, pp. 47-57.

POULLET Y., «Protection des données à caractère personnel et obligation de sécurité », dans *La sécurité informatique, entre technique et droit*, Bruxelles, Story-Scientia, 1998. - pp. 195-224.

REVEILLON A., « La e-surveillance des employés. Le contrôle des e-mails et des sites visités », *Ubiquité*, 2002, n°11, pp. 33-53.

ROBBEN F. MAES P., La Banque carrefour de la Sécurité sociale comme moteur de l'e-governement du secteur social, 2006, disponible sur *http://www.ksz-bcss.fgov.be/documentation/fr/documentation/presse/LaBCSS*

TRUDEL P., ABRAN F. Guide pour un usage responsable d'Internet. A l'intention des responsables des lieux d'accès publics à Internet et des utilisateurs, 2003, disponible sur *http : //www.crdp.umontreal.ca/guides/nonscol.pdf*

Rapport de recherche

BURTON C., LAURENT V., LOBET-MARIS C., NAVARRE F., POULLET Y., « L'informatisation des CPAS, une informatique plurielle au service de l'action sociale », Résultats du questionnaire préparatoire au Colloque des Secrétaires de CPAS, Herbeumont, avril 2006, rapport disponible sur *http://www.fundp.ac.be/pdf/publications/57376.pdf*